

INTERACTIVE FUNCTION COMPUTATION VIA POLAR CODING

TALHA CIHAD GULCU* AND ALEXANDER BARG**

ABSTRACT. In a series of papers N. Ma and P. Ishwar (2011-13) considered a range of distributed source coding problems that arise in the context of iterative computation of functions, characterizing the region of achievable communication rates. We consider the problems of interactive computation of functions by two terminals and interactive computation in a collocated network, showing that the rate regions for both these problems can be achieved using several rounds of polar-coded transmissions.

1. INTRODUCTION

Interactive computation in networks has been recently attracting attention of researchers in information theory and computer science alike. Aspects of interactive computation have been analyzed from various perspectives including establishing the region of achievable rates, complexity and security of computations, as well as a number of other problems [4, 5, 6, 16, 21].

A line of work starting with the paper [11] examined the question of computing a function $f(X, Y)$ where X is a discrete memoryless source and Y represents side information provided to the decoder as a random variable correlated with X . The main question addressed in these works is whether communication for computing the function rather than communicating the source itself can reduce the volume of transmission. While [11] confined itself to the modulo-two sum of X and Y , later works, e.g., [17] extended the problem to arbitrary functions f , finding the region of achievable rates for one or two rounds of communication for computing f .

In this work we focus on the problems considered in [12, 14] which generalize the setting of [17] to multiple rounds of communication. The main problem considered in these papers concerns the scenario in which two terminals observe multiple independent realizations of correlated random variables. The objective of the terminals is to establish and conduct communication that enables them to compute a function of their observations. An obvious solution is to transmit the entire sequence of observations from Terminal A to Terminal B and the same in the reverse direction whereupon the computation can be trivially completed. The problem considered in the cited works is to reduce the amount of transmitted information using ideas from distributed lossy compression, thereby reducing the problem to a version of distributed source coding. An extension of this problem considered in [14] concerns transmission in a multiterminal network where the computation is performed by a single dedicated node. In both scenarios the cited papers characterized exactly the region of achievable rates of communication for the function computation.

Starting with the results of [12, 14], in this paper we design explicit communication protocols that achieve the rate regions of the two communication models discussed above. In our schemes, communication is performed by exchanging several messages between the terminals formed by using the ideas related to Arkan's polar coding scheme [2]. Polar codes were initially introduced for transmission over binary-input discrete memoryless channels [2]. They were subsequently applied in a variety of situations related to communication and data compression. In particular, it is possible to modify the original scheme to achieve the optimal compression rate in the problem of lossless coding of memoryless discrete sources as well as a distributed version of this problem (the Slepian-Wolf problem) [1]. It is also possible to design a polar-coding scheme for lossy source coding, including Wyner-Ziv's distributed version of this problem [9, 10]. As shown in these works, it is possible to compress a discrete memoryless source using polar codes, attaining the compression rate that approaches the (symmetric) rate-distortion function of the source.

These results serve a starting point of our research which also proceeds in the context of distributed lossy compression. The new challenges in our constructions arise from the fact that for function computation we need to implement

Date: November 3, 2015.

* Department of ECE and Institute for Systems Research, University of Maryland, College Park, MD 20742, Email: gulcu@umd.edu. Research supported in part by NSF grant CCF1217245.

** Department of ECE and Institute for Systems Research, University of Maryland, College Park, MD 20742, and IITP, Russian Academy of Sciences, Moscow, Russia. Email: abarg@umd.edu. Research supported in part by NSF grants CCF1217894, CCF1217245, and CCF1422955. Email: abarg@umd.edu.

an interactive scheme. The problem extends beyond using several rounds of the lossy compression scheme because neither the coding of [10] nor its analysis generalize immediately to multiple rounds. To proceed, we bring in an idea in another recent work on polar codes, [8], devoted to their extension to asymmetric channels. Recall that the original polar coding scheme [2] involves data bits together with “frozen bits” whose values are shared with the decoder. Paper [8] further refines this partition, introducing three types of coordinates based on their conditional entropies. We modify this idea, defining a partition that ensures the validity of our interactive communication scheme. This setup, however, comes at a price of more involved analysis, which we proceed to discuss.

Recall that the main challenge in proving that polar codes attain the rate-distortion function consisted in showing that the joint statistic of the source sequence and the polar-compressed sequence is close to the “ideal” statistic arising from the rate-distortion theorem [10]. Estimates of this kind form the main technical contents of our research, and lie in the core of the proofs. Our situation however is more difficult than the setting of distributed compression because we need to show that the mentioned statistic is close to the ideal distribution both for the transmitting and receiving parties. It may seem that the transmitter already has all the information, and there is no reason that it cannot recover the data with high probability or even probability one. This is not the case because the interactive nature of the communication protocol calls for a different encoding procedure of polar codes. To define it, we introduce a partition of the data block into message bits, random bits, and near-deterministic bits. This supports the required functionality, but at the same time biases the joint statistic. For this reason, to prove proximity of the distributions even in the first round, we have to rely on rather involved induction arguments, analyzing separately the observations of the transmitter and the receiver. At a high level, we need to show that both terminals generate the same sequence of random variables with high probability, leading to the reliable computation of their functions. Proofs of the described claims take up a large part of the paper. These ideas are developed in Sect. 4.1, 4.2; see in particular Lemmas 4 and 5.

Once the needed properties of the distributions are established for the first round, we proceed to extend the argument to multiple rounds of communication. Namely, in Sect. 4.3, 4.4 we show that after several rounds of communication at rates that approach the optimal rate for this problem, the terminals recover the random sequences generated by each other with high probability. This is proved via another induction argument which has to take account of multiple Markov chain conditions that arise naturally in the course of the exchange.

Our overall goal is accomplished in Sect. 4.5 where we prove that the desired function values are computed by the terminals with probability approaching one. To complete the discussion, in Sect. 4.6 we give an example of distributed computation where our scheme provides a gain in the amount of transmitted data over sending the realizations of the random variables observed by the terminals.

Finally, in Sect. 5 we show that the designed protocol can be extended to a version of distributed computation performed in a network of terminals [14]. It turns out that our scheme for two terminals can be modified to attain optimal rates of communication for this scenario. The main elements of the analysis are similar to the case of two terminals.

In summary, we suggest a version of polar codes that support the primitive of interactive lossy source coding and apply it to some function computation problems. This takes interactive source coding one step closer towards practicality by showing that polar codes, which are known to have near linear coding complexity, can indeed recover the rate regions. We also introduce some new technical tools that could be useful in other interactive communication schemes based on polar codes.

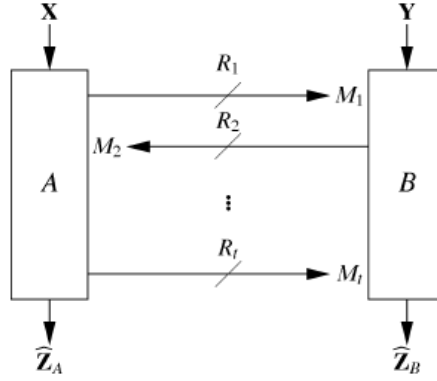
2. PROBLEM STATEMENT

2.1. Two-terminal network. The interactive distributed source coding problem that we consider in this paper is illustrated in Figure 1. Let X and Y be discrete random variables taking values in finite sets (alphabets) \mathcal{X} and \mathcal{Y} and let p_{XY} be their joint distribution. Suppose that we are given N independent realizations

$$(X, Y)^{1:N} = ((X(1), Y(1)), (X(2), Y(2)), \dots, (X(N), Y(N)))$$

of the pair (X, Y) (here and elsewhere a vector of the form (X^i, \dots, X^j) is abbreviated as $X^{i:j}$). We assume that Terminal A observes the sequence $X^{1:N} \in \mathcal{X}^N$ and Terminal B observes the sequence $Y^{1:N} \in \mathcal{Y}^N$.

The aim of Terminal A is to calculate the function $f_A : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}_A$ for indices $i = 1, \dots, N$. Similarly, the aim of Terminal B is to calculate the function $f_B : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}_B$, where $\mathcal{Z}_A, \mathcal{Z}_B$ are some finite alphabets. In other words, Terminals A and B attempt to compute $Z_A^{1:N} \triangleq (Z_A(1), Z_A(2), \dots, Z_A(N))$ and $Z_B^{1:N} \triangleq (Z_B(1), Z_B(2), \dots, Z_B(N))$ respectively, where $Z_A(i) = f_A(X(i), Y(i))$ and $Z_B(i) = f_B(X(i), Y(i))$, for $i = 1, \dots, N$.

FIGURE 1. Interactive distributed source coding with t alternating messages.

Definition 1. A two-terminal t -round interactive source code with the parameters $(t, N, |\mathcal{M}_1|, \dots, |\mathcal{M}_t|)$ is formed by t encoding functions e_1, \dots, e_t and two block decoding functions g_A, g_B of blocklength N such that

$$(\text{Enc } j, j = 1, \dots, t) \quad e_j : \begin{cases} \mathcal{X}^N \times \bigotimes_{i=1}^{j-1} \mathcal{M}_i \rightarrow \mathcal{M}_j & \text{if } j \text{ is odd} \\ \mathcal{Y}^N \times \bigotimes_{i=1}^{j-1} \mathcal{M}_i \rightarrow \mathcal{M}_j & \text{if } j \text{ is even} \end{cases}$$

$$(\text{Dec A}) \quad g_A : \mathcal{X}^N \times \bigotimes_{j=1}^t \mathcal{M}_j \rightarrow \mathcal{Z}_A^N$$

$$(\text{Dec B}) \quad g_B : \mathcal{Y}^N \times \bigotimes_{j=1}^t \mathcal{M}_j \rightarrow \mathcal{Z}_B^N.$$

Without loss of generality we are assuming that communication is initiated by Terminal A. The value of the encoder mapping e_j is called the j th message (of A or B, as appropriate) and denoted by $M_j, j = 1, \dots, t$, where t is the total number of messages in the protocol. The outputs of the decoders A and B are denoted by $\hat{Z}_A^{1:N}$ and $\hat{Z}_B^{1:N}$, respectively.

Definition 2. A rate tuple $\mathbf{R} = (R_1, \dots, R_t)$ is achievable for t -round interactive function computation if for every $\epsilon > 0$ there exists $N(\epsilon, t)$ such that for all $N > N(\epsilon, t)$, there exists a two-terminal interactive source code with the parameters $(t, N, |\mathcal{M}_1|, \dots, |\mathcal{M}_t|)$ such that

$$\begin{aligned} \frac{1}{N} \log_2 |\mathcal{M}_j| &\leq R_j + \epsilon, \quad j = 1, \dots, t \\ \Pr(Z_A^{1:N} \neq \hat{Z}_A^{1:N}) &\leq \epsilon, \quad \Pr(Z_B^{1:N} \neq \hat{Z}_B^{1:N}) \leq \epsilon. \end{aligned}$$

The set of all achievable rate tuples is denoted by \mathcal{R}_t^A .

Theorem 1. [12] A t -tuple of rate values \mathbf{R} is contained in the region of achievable rates \mathcal{R}_t^A if and only if there exist random variables $U^{1:t} = (U^1, \dots, U^t)$ such that for all $i = 1, \dots, t$

$$\begin{aligned} R_i &\geq \begin{cases} I(X; U^i | Y, U^{1:i-1}), & U^i \rightarrow (X, U^{1:i-1}) \rightarrow Y, \quad i \text{ odd} \\ I(Y; U^i | X, U^{1:i-1}), & U^i \rightarrow (Y, U^{1:i-1}) \rightarrow X, \quad i \text{ even} \end{cases} \\ H(f_A(X, Y) | X, U^{1:t}) &= 0, \quad H(f_B(X, Y) | Y, U^{1:t}) = 0 \end{aligned} \tag{1}$$

where the auxiliary random variables $U^{1:t}$ are supported on finite sets \mathcal{U}^i such that

$$|\mathcal{U}^j| \leq \begin{cases} |\mathcal{X}|(\prod_{i=1}^{j-1} |\mathcal{U}^i|) + t - j + 3, & j \text{ odd} \\ |\mathcal{Y}|(\prod_{i=1}^{j-1} |\mathcal{U}^i|) + t - j + 3, & j \text{ even}. \end{cases} \tag{2}$$

The conditions of entropy being equal to zero in this theorem simply reflect the fact that f_A (or f_B) is a deterministic function of $X, U^{1:t}$ (or $Y, U^{1:t}$), and no additional randomness is involved in its evaluation. Finding the auxiliary

random variables U^1, U^2, \dots, U^t that satisfy the conditions of this theorem for a given pair of functions f_A, f_B is a separate question which is addressed on a case-by-case basis.

Of course, the main question associated with this result, before we even try to construct an explicit scheme that aims at attaining this rate region, is whether the communication protocol implied by this theorem results in overall saving in communication compared to a straightforward transmission of X to B and Y to A . The answer is positive at least in some examples [12]. We discuss one of them below in this paper; see Sect. 4.6.

2.2. Multiterminal collocated networks. Ma, Ishwar, and Gupta [14] also considered a multiterminal extension of the problem described in the previous section. To describe it, consider a network with m source terminals and a single sink terminal. Each source terminal j observes a random sequence $(X^j)^{1:N} = (X^j(1), \dots, X^j(N)) \in \mathcal{X}_j^N, j = 1, \dots, m$. Unlike the two-terminal case, the sources are assumed to be independent, i.e., for any $i \in [N]$, the random variables $(X^1(i), X^2(i), \dots, X^m(i))$ satisfy

$$P_{X^{1:m}}(x^{1:m}) = \prod_{j=1}^m P_{X^j}(x^j).$$

Let $f : \mathcal{X}_1 \times \dots \times \mathcal{X}_m \rightarrow \mathcal{Z}$ be the function that the sink terminal aims to compute. In other words, the purpose of this terminal is to compute the sequence $Z^{1:N} = (Z(1), \dots, Z(N))$, where $Z(i) \triangleq f(X^1(i), X^2(i), \dots, X^m(i))$ is the i^{th} coordinate of the function.

We assume that communication is initiated by Terminal 1. The terminals take turns to broadcast messages in t steps. Every broadcasted message is recovered correctly by every terminal. Based on all the t messages transmitted, the sink node computes $Z^{1:N}$. If $t > m$, the communication is called interactive.

Definition 3. A t -message distributed source code in a collocated network with parameters $(t, N, |\mathcal{M}_1|, \dots, |\mathcal{M}_t|)$ is a collection of t encoding functions e_1, \dots, e_t and a decoding function g , where for every $i \in [t]$, $j = (i-1) \bmod m + 1$

$$e_i : (\mathcal{X}^j)^N \times \bigotimes_{l=1}^{i-1} \mathcal{M}_l \rightarrow \mathcal{M}_i, \quad g : \bigotimes_{l=1}^t \mathcal{M}_l \rightarrow \mathcal{Z}^N.$$

The output of the encoder e_i is called the i^{th} message. The output of the decoder is denoted by $\hat{Z}^{1:N}$.

Definition 4. A rate tuple $\mathbf{R} = (R_1, \dots, R_t)$ is achievable for t -round function computation in a collocated network if for all $\epsilon > 0$ there exists $N(\epsilon, t)$ such that for every $N > N(\epsilon, t)$, there exists a t -message distributed source code with the parameters $(t, N, |\mathcal{M}_1|, \dots, |\mathcal{M}_t|)$ such that

$$\frac{1}{N} \log_2 |\mathcal{M}_i| \leq R_i + \epsilon, \quad i = 1, \dots, t, \\ P(Z^{1:N} \neq \hat{Z}^{1:N}) \leq \epsilon.$$

The set of all achievable rate tuples is denoted by \mathcal{R}_t .

Theorem 2. [14] For $i = 1, \dots, t$ let

$$D_i = \{R_i : R_i \geq I(X^j; U^i | U^{1:i-1}) \text{ for all } j = (i-1) \bmod m + 1\}. \quad (3)$$

For all $t \in \mathbb{N}$, we have

$$\mathcal{R}_t = \bigcup_{P_{U^{1:t}|X^{1:m}}} \{\mathbf{R} = (R_1, \dots, R_t) | R_i \in D_i, i \in [t]\} \quad (4)$$

where the union is over the distributions $P_{U^{1:t}|X^{1:m}}$ that satisfy the following conditions:

- (i) $H(f(X^{1:m}) | U^{1:t}) = 0$,
- (ii) For every $i \in [t]$, $j = (i-1) \bmod m + 1$, $U^i \rightarrow (U^{1:i-1}, X^j) \rightarrow (X^{1:j-1}, X^{j+1:m})$ is a Markov chain;
- (iii) The cardinalities of the alphabets of the auxiliary random variables $U^{1:t}$ are bounded above as in (2).

A polar-coded scheme that attains this rate region is presented in Sect. 5.

3. PRELIMINARIES ON POLAR CODING

We begin with recalling basic notation for polar codes. For a binary random variable T and a discrete random variable V supported on \mathcal{V} define the Bhattacharyya parameter as follows:

$$Z(T|V) = 2 \sum_{v \in \mathcal{V}} P_V(v) \sqrt{P_{T|V}(0|v)P_{T|V}(1|v)}.$$

If $P_T(0) = P_T(1) = 1/2$, then this definition coincides with the usual definition of the Bhattacharyya parameter for the communication channel $T \rightarrow V$. The value $Z(T|V)$, $0 \leq Z(T|V) \leq 1$ measures the amount of randomness in T given V in the sense that if it is close to zero, then T is almost constant, while if it is close to one, then T is almost uniform in $\{0, 1\}$.

For $N = 2^n$ and $n \in \mathbb{N}$, the polarizing matrix (or the Arıkan transform matrix) is defined as $G_N = B_N F^{\otimes n}$, where $F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, \otimes is the Kronecker product of matrices, and B_N is a “bit reversal” permutation matrix [2]. In his landmark paper [2], Arıkan showed that given a binary channel W , an appropriate subset of the rows of G_N can be used as a generator matrix of a linear code that approaches the symmetric capacity of W as $N \rightarrow \infty$.

3.1. Source coding. Let X be a binary memoryless source, let $X^{1:N}$ denote N independent copies of X , and let $U^{1:N} = X^{1:N} G_N$. Define subsets $\mathcal{H}_X = \mathcal{H}_{X,N}$ and $\mathcal{L}_X = \mathcal{L}_{X,N}$ of $[N]$ as follows:

$$\begin{aligned} \mathcal{H}_X &= \{i \in [N] : Z(U^i | U^{1:i-1}) \geq 1 - \delta_N\} \\ \mathcal{L}_X &= \{i \in [N] : Z(U^i | U^{1:i-1}) \leq \delta_N\} \end{aligned} \tag{5}$$

where $\delta_N \triangleq 2^{-N^\beta}$, $\beta \in (0, 1/2)$. (The choice of this particular value of δ_N is related to the convergence rate of the polarizing process [3].) Note that each bit U_i , $i \in \mathcal{L}_X$ is nearly deterministic given the values $U^{1:i-1}$, while the bits in \mathcal{H}_X are nearly uniformly random. As shown in [1], the proportion of indices $i \in [N]$ that are contained in \mathcal{H}_X approaches $H(X)$, and the proportion of bits that are not polarized (i.e., are in $(\mathcal{H}_X \cup \mathcal{L}_X)^c$) behaves as $o(N)$. Therefore, as $N \rightarrow \infty$, the source sequence $x^{1:N}$ can be recovered with high probability from $NH(X)$ bits in \mathcal{H}_X .

Suppose further that there is a random variable Y with a joint distribution P_{XY} with the source (Y is often called the side information about X). Similarly to (5) define

$$\begin{aligned} \mathcal{H}_{X|Y} &= \{i \in [N] : Z(U^i | U^{1:i-1}, Y^{1:N}) \geq 1 - \delta_N\} \\ \mathcal{L}_{X|Y} &= \{i \in [N] : Z(U^i | U^{1:i-1}, Y^{1:N}) \leq \delta_N\}. \end{aligned} \tag{6}$$

Suppose again that the polarizing transformation is applied to $X^{1:N}$. It can be shown that [1, 9]

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{1}{N} |\mathcal{H}_{X|Y}| &= H(X|Y) \\ \lim_{N \rightarrow \infty} \frac{1}{N} |\mathcal{L}_{X|Y}| &= 1 - H(X|Y). \end{aligned}$$

In other words, using polarization the source can be compressed to $NH(X|Y)$ bits. This setting is useful, for instance, in distributed lossless compression where the correlation between the observations of two terminals plays the role of the side information. Note that $Z(U_i | U^{1:i-1}, Y^{1:N}) \leq Z(U_i | U^{1:i-1})$ and therefore,

$$\begin{aligned} \mathcal{H}_{X|Y} &\subseteq \mathcal{H}_X \\ \mathcal{L}_X &\subseteq \mathcal{L}_{X|Y}. \end{aligned} \tag{7}$$

3.2. Channel coding. Let $W(Y|X)$ be a binary-input discrete memoryless channel with capacity achieving distribution P_X . In the case of uniform P_X , [3] showed that n iterations of the transform with kernel F polarize the transmitted bits into an almost deterministic subset $N_d \subset [N]$ and an almost random subset $N_r \subset [N]$ so that $|N_d| \rightarrow NI(X; Y)$ as $n \rightarrow \infty$. This construction was extended in [8] to cover the case of arbitrary distributions P_X (see also a discussion of this construction in [15]). They observed that if the bits in $\mathcal{H}_X \setminus \mathcal{L}_{X|Y}$ are known to the decoder, the remaining bits are likely to be contained in $\mathcal{L}_{X|Y}$, and can be recovered correctly with high probability from the channel output $y^{1:N}$ and previously found bits using the successive decoding procedure. This shows that the number of bits that carry information equals $N(H(X) - H(X|Y)) = NI(X; Y)$. We refer to [8] for further details.

4. THE ANALYSIS OF POLAR CODES FOR INTERACTIVE FUNCTION COMPUTATION PROBLEM

In this section we show that the rate region (1) of the two-terminal function computation is achievable via polar coding. The overall idea is to transmit the value of the auxiliary random variables U^i in their respective rounds of communication; see Theorem 1. This is done interactively by alternating the roles of the transmitter and the receiver between the terminals. Upon completion of the communication, both terminals have the realizations of the U^i s, and their respective values coincide with high probability. The random variables associated with these realizations are denoted by U_A^i and U_B^i below. Once the desired properties of these random variables are established, the actual function computation is accomplished relying on the conditional entropy constraints in (1).

In the first part of our presentation (Sections 4.1 and 4.2), we describe and analyze the first round of communication between the terminals. As already mentioned, we will need to show that the joint distributions of U_A^1 and the observations of the terminals given by the random variables X, Y are close to the ideal distribution $P_{(U^1)^{1:N}, X^{1:N}, Y^{1:N}}$. The reason that this needs to be proved for the transmitter terminal (Terminal A in Round 1) is discussed in the Introduction in general terms. In greater detail, it stems from the fact that, apart from the data bits, we also have a subblock of low-entropy (nearly deterministic) bits encoded into the vector U_A^1 . This entails the need for a careful analysis of the empirical probability distribution, which is performed in Lemma 4.

Once this is accomplished, we move to the analysis of the data received by Terminal B. We need to show that its version of the realization of U^1 equals U_A^1 with high probability. To prove this, we would like to make use of the proximity of the joint statistics to the ideal distribution, but this fact itself requires a proof. Thus, we are faced with proving two concurrent and mutually interdependent estimates. This question is resolved by an induction argument that gets rather technical and relies on delicate estimates of the distance between various distributions and on Markov chain conditions. This argument forms the contents of Lemma 5 below.

The next step is to generalize the claim for Round 1 to multiple rounds. This part is relatively easier, but still new to the analysis of polar codes because of accounting for multiple Markov chain conditions. It is contained in Sect. 4.4. To conclude the proof, we show in Sect. 4.5 that each terminal correctly computes its function value with a probability converging to 1.

Let U^1, \dots, U^t be random variables that satisfy the Markov chain conditions and conditional entropy conditions of Theorem 1. Throughout the section, P_{XYU^1} and $P_{XYU^{1:t}}$ refer to the joint distribution of the random variables X, Y, U^1 and X, Y, U^1, \dots, U^t , respectively. We will also assume that all the random variables U^1, \dots, U^t are binary. Generalizations to the case of a nonbinary alphabet can be easily accomplished using a multitude of methods available in the literature. Finally, to simplify the notation, in this section we use $\bar{\cdot}$ to refer to N -vectors: for instance, $\bar{X} = X^{1:N}$, $\bar{u}_A^1 = (u_A^1)^{1:N}$, etc. For vectors of other dimensions we retain the original notation, e.g., $(u_A^1)^{1:i} = (u_A^1(1), \dots, u_A^1(i))$, etc.

4.1. First round of communication. We begin with a detailed discussion of the first round of communication, i.e., the round in which A transmits to B a message from its set of 2^{NR_1} messages. We begin with a detailed discussion of the first round of communication, i.e., the round in which A transmits to B a message from its set of 2^{NR_1} messages.

Consider the joint distribution

$$P_{V^1 \bar{X} \bar{Y} \bar{U}^1}(\bar{v}^1, \bar{x}, \bar{y}, \bar{u}^1) = \mathbb{1}(\bar{u}^1 G_N = \bar{v}^1) \prod_{i=1}^N P_{XYU^1}(x^i, y^i, (u^1)^i).$$

Various marginal and conditional distributions used below, denoted by P , are assumed to be implied by this expression. The purpose of the first round of communication is to make it possible for both terminals to generate the random vector \bar{U}^1 so that the joint distribution of $\bar{U}^1, \bar{X}, \bar{Y}$ is close to $P_{\bar{U}^1 \bar{X} \bar{Y}}$.

Consider the following partition:

$$\left. \begin{aligned} \mathcal{F}_r &= \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1|X} \\ \mathcal{F}_d &= \mathcal{L}_{U^1} \\ \mathcal{I} &= \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1|X}^c \end{aligned} \right\} \quad (8)$$

Remark: For readers familiar with [8] we note that this partition, while inspired by this paper, is different from the one used in it. Our choice is better suited for the analysis of joint statistics of the observations and the auxiliary random variables that arise in the present study.

Round 1: The transmission scheme in the first round of communication pursues the goal of sharing the sequence \bar{u}^1 between the two terminals. This goal is accomplished using the following procedure. Given \bar{x} , Terminal A computes the sequence \bar{v}_A^1 in a successive fashion by sampling from the conditional distribution

$$Q_{(V_A^1)^i|(V_A^1)^{1:i-1}\bar{X}}((v_A^1)^i|(v_A^1)^{1:i-1}, \bar{x}) = \begin{cases} 1/2, & i \in \mathcal{F}_r \\ P_{(V^1)^i|(V^1)^{1:i-1}}((v_A^1)^i|(v_A^1)^{1:i-1}), & i \in \mathcal{F}_d \\ P_{(V^1)^i|(V^1)^{1:i-1}\bar{X}}((v_A^1)^i|(v_A^1)^{1:i-1}, \bar{x}), & i \in \mathcal{I}. \end{cases} \quad (9)$$

Once \bar{v}_A^1 is found, Terminal A transmits $(v_A^1)^i$ to Terminal B. Note that the bits in the subset $\mathcal{L}_{U^1}^c \cap \mathcal{L}_{U^1|Y}$ can be recovered by B with high probability based on its own observations. For this reason, A transmits only the subvector of \bar{v}_A^1 whose coordinate indices satisfy

$$i \in \mathcal{I}' \triangleq \mathcal{I} \setminus (\mathcal{L}_{U^1}^c \cap \mathcal{L}_{U^1|Y}). \quad (10)$$

After observing \bar{y} and receiving $(v_A^1)^i, i \in \mathcal{I}'$ from Terminal A, Terminal B calculates $(v_B^1)^i, i \in (\mathcal{I}')^c$ in a probabilistic way by sampling from the distribution

$$Q_{(V_B^1)^i|(V_B^1)^{1:i-1}\bar{Y}}((v_B^1)^i|(v_B^1)^{1:i-1}, \bar{y}) = \begin{cases} 1/2, & i \in \mathcal{F}_r \\ P_{(V^1)^i|(V^1)^{1:i-1}}((v_B^1)^i|(v_B^1)^{1:i-1}), & i \in \mathcal{F}_d \\ P_{(V^1)^i|(V^1)^{1:i-1}\bar{Y}}((v_B^1)^i|(v_B^1)^{1:i-1}, \bar{y}), & i \in \mathcal{I} \setminus \mathcal{I}'. \end{cases} \quad (11)$$

Since $(v_B^1)^i = (v_A^1)^i$ for all $i \in \mathcal{I}'$, Terminal B can form the sequence \bar{v}_B . It then computes \bar{u}_B^1 by performing the multiplication $\bar{u}_B^1 = \bar{v}_B^1 G_N$. Terminal A also computes its version of the sequence \bar{u}^1 by finding $\bar{u}_A^1 = \bar{v}_A^1 G_N$.

4.2. Analysis of the first round of communication. First let us show that the rate of the first round of communication approaches the limiting value given in Theorem 1.

Lemma 3. *The rate of the first round of communication tends to $I(X; U^1|Y)$ as N goes to infinity.*

Proof. Since $\mathcal{L}_{U^1} \subseteq \mathcal{L}_{U^1|Y}$ (7), it follows that

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{|\mathcal{L}_{U^1}^c \cap \mathcal{L}_{U^1|Y}|}{N} &= \lim_{N \rightarrow \infty} \left(\frac{|\mathcal{L}_{U^1|Y}|}{N} - \frac{|\mathcal{L}_{U^1}|}{N} \right) \\ &= (1 - H(U^1|Y)) - (1 - H(U^1)) \\ &= I(U^1; Y). \end{aligned}$$

Moreover, the Markov chain condition $U^1 \rightarrow X \rightarrow Y$ imposed by Theorem 1 implies the inclusion $\mathcal{L}_{U^1|Y} \subseteq \mathcal{L}_{U^1|X}$. (See Lemma 4.7 of [9] for the proof.) Therefore, as the blocklength N goes to infinity, the rate of the first round of communication converges to

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{|\mathcal{I}|}{N} - I(U^1; Y) &= I(U^1; X) - I(U^1; Y) \\ &= (H(U^1) - H(U^1|X)) - (H(U^1) - H(U^1|Y)) \\ &= H(U^1|Y) - H(U^1|X) \\ &= H(U^1|Y) - H(U^1|X, Y) \\ &= I(X; U^1|Y) \end{aligned} \quad (12)$$

as desired, where (12) again follows from the Markov condition. \square

As already discussed, the main technical obstacle is to show that the joint statistics of the observations and the auxiliary random variables are close to the ideal statistic. More specifically, we need to prove that the joint distributions of both $\bar{U}_A^1, \bar{X}, \bar{Y}$ and $\bar{U}_B^1, \bar{X}, \bar{Y}$ are close to $P_{\bar{U}^1 \bar{X} \bar{Y}}$, and in fact $\bar{U}_A^1 = \bar{U}_B^1$ holds true with probability converging to 1.

Let $Q_{\bar{U}_A^1 \bar{X} \bar{Y}}(\bar{u}_A^1, \bar{x}, \bar{y})$ denote the probability that Terminal A observes the source sequence \bar{x} , Terminal B observes the source sequence \bar{y} , and the procedure described by (9) outputs \bar{u}_A^1 .

Lemma 4. For any $\beta_1 < \beta \in (0, 1/2)$, starting with some N we have

$$\|Q_{\bar{U}_A^1 \bar{X} \bar{Y}} - P_{\bar{U}^1 \bar{X} \bar{Y}}\|_1 = O(2^{-N^{\beta_1}}).$$

The proof is given in Appendix A.

Now we turn to the information processing by Terminal B described above (see (11)). Let

$$Q_{\bar{U}_B^1 \bar{X} \bar{Y}}(\bar{u}_B^1, \bar{x}, \bar{y})$$

denote the probability that Terminals A and B observe the source sequences \bar{x} and \bar{y} respectively, and the described procedure outputs \bar{u}_B^1 . Then Terminal B's counterpart of Lemma 4 can be stated as follows.

Lemma 5. For any $\beta_2 < \beta \in (0, 1/2)$, starting with some N we have

$$\|Q_{\bar{U}_B^1 \bar{X} \bar{Y}} - P_{\bar{U}^1 \bar{X} \bar{Y}}\|_1 = O(2^{-N^{\beta_2}}) \quad (13)$$

$$\Pr\{\bar{U}_A^1 = \bar{U}_B^1\} = 1 - O(2^{-N^{\beta_2}}). \quad (14)$$

Remark: The statement that we need below is given by (14). However, both claims (13) and (14) are used in the proof (recall the discussion in the introduction to this section).

The proof is given in Appendix B.

4.3. The remaining rounds of communication. The purpose of this round to make it possible for both terminals to generate the random vector \bar{U}^{i+1} so that the joint distribution of $\bar{U}^{i+1}, \bar{X}, \bar{Y}$ is close to the ideal distribution $P_{\bar{U}^{i+1} \bar{X} \bar{Y}}$.

The communication protocol of the first round easily generalizes to the remaining rounds of communication. Consider for instance round $i + 1$, where i is even. This means that information is communicated from A to B, and that sequences $\mathbf{u}^{1:i} \triangleq (\bar{u}^1, \dots, \bar{u}^i)$ are already known to both sides.

Below we use notation P for the joint distribution

$$\begin{aligned} P_{\mathbf{U}^{1:t} \mathbf{V}^{1:t} \bar{X} \bar{Y}}(\mathbf{u}^{1:t}, \mathbf{v}^{1:t}, \bar{x}, \bar{y}) \\ = \prod_{j=1}^N P_{XYU^{1:t}}(x^j, y^j, (u^1)^j, \dots, (u^t)^j) \prod_{i=0}^{t-1} \mathbb{1}(\bar{u}^{i+1} G_N = \bar{v}^{i+1}) \end{aligned} \quad (15)$$

and distributions derived from it, where $\mathbf{V}^{1:t} \triangleq (\bar{V}^1, \dots, \bar{V}^t)$, $\mathbf{U}^{1:t} \triangleq (\bar{U}^1, \dots, \bar{U}^t)$. We assume that no errors occurred in earlier rounds, so both terminals observe identical copies of $\mathbf{u}^{1:i}$.

Round $i + 1$ (i even): Terminal A partitions $[N]$ as follows:

$$\left. \begin{aligned} \mathcal{F}_r^{i+1} &= \mathcal{L}_{U^{i+1}}^c \cap \mathcal{H}_{U^{i+1}|(X, U^{1:i})} \\ \mathcal{F}_d^{i+1} &= \mathcal{L}_{U^{i+1}} \\ \mathcal{I}^{i+1} &= \mathcal{L}_{U^{i+1}}^c \cap \mathcal{H}_{U^{i+1}|(X, U^{1:i})} \end{aligned} \right\} \quad (16)$$

It then generates a sequence \bar{v}_A^{i+1} randomly and successively by sampling from the distribution

$$\begin{aligned} Q_{(V_A^{i+1})^j | (V_A^{i+1})^{1:j-1}, (\bar{X}, \mathbf{U}^{1:i})}((v_A^{i+1})^j | (v_A^{i+1})^{1:j-1}, (\bar{x}, \mathbf{u}^{1:i})) \\ = \begin{cases} 1/2, & j \in \mathcal{F}_r^{i+1} \\ P_{(V^{i+1})^j | (V^{i+1})^{1:j-1}}((v_A^{i+1})^j | (v_A^{i+1})^{1:j-1}), & j \in \mathcal{F}_d^{i+1} \\ P_{(V^{i+1})^j | (V^{i+1})^{1:j-1}, (\bar{X}, \mathbf{U}^{1:i})}((v_A^{i+1})^j | (v_A^{i+1})^{1:j-1}, (\bar{x}, \mathbf{u}^{1:i})), & j \in \mathcal{I}^{i+1}. \end{cases} \end{aligned} \quad (17)$$

Having found \bar{v}_A^{i+1} , Terminal A computes the sequence $\bar{u}_A^{i+1} = \bar{v}_A^{i+1} G_N$.

To communicate information, A sends to B the sequence $(v_A^{i+1})^j, j \in \mathcal{I}'$, where (16)

$$\mathcal{I}'^{i+1} = \mathcal{I}^{i+1} \setminus (\mathcal{L}_{U^{i+1}}^c \cap \mathcal{L}_{U^{i+1}|(Y, U^{1:i})}).$$

Upon receiving the transmission, Terminal B generates $(v_B^{i+1})^j, j \notin \mathcal{I}'$ by sampling from the distribution

$$\begin{aligned} Q_{(V_B^{i+1})^j | (V_B^{i+1})^{1:j-1}, (\bar{Y}, \mathbf{U}^{1:i})}((v_B^{i+1})^j | (v_B^{i+1})^{1:j-1}, (\bar{y}, \mathbf{u}^{1:i})) \\ = \begin{cases} 1/2, & j \in \mathcal{F}_r, \\ P_{(V^{i+1})^j | (V^{i+1})^{1:j-1}}((v_B^{i+1})^j | (v_B^{i+1})^{1:j-1}), & j \in \mathcal{F}_d, \\ P_{(V^{i+1})^j | (V^{i+1})^{1:j-1}, (\bar{Y}, \mathbf{U}^{1:i})}((v_B^{i+1})^j | (v_B^{i+1})^{1:j-1}, (\bar{y}, \mathbf{u}^{1:i})), & j \in \mathcal{I}^{i+1} \setminus \mathcal{I}'^{i+1}. \end{cases} \end{aligned} \quad (18)$$

The values $(v_B^{i+1})^j, j \in \mathcal{I}^{i+1}$ are known perfectly from the communication. Once the sequence \bar{v}_B^{i+1} has been formed, Terminal B finds $\bar{u}_B^{i+1} = \bar{v}_B^{i+1} G_N$.

If i is odd, the transmission proceeds from Terminal B to A. Both the description of the information processing and the analysis below apply after obvious changes of notation.

Let us show that the rate of $(i+1)^{\text{th}}$ round of communication matches the lower bound of R_{i+1} given in (1).

Lemma 6. *If $i+1$ is odd, the rate of the $(i+1)^{\text{th}}$ round converges to $I(X; U^i | Y, U^{1:i-1})$ as N goes to infinity. If $i+1$ is even, the rate converges to $I(Y; U^i | X, U^{1:i-1})$.*

Proof. Since $\mathcal{L}_{U^{i+1}} \subseteq \mathcal{L}_{U^{i+1}|(Y, U^{1:i})}$, we have

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{|\mathcal{L}_{U^{i+1}}^c \cap \mathcal{L}_{U^{i+1}|(Y, U^{1:i})}|}{N} &= \lim_{N \rightarrow \infty} \left(\frac{|\mathcal{L}_{U^{i+1}|(Y, U^{1:i})}|}{N} - \frac{|\mathcal{L}_{U^{i+1}}|}{N} \right) \\ &= (1 - H(U^{i+1} | Y, U^{1:i})) - (1 - H(U^{i+1})) \\ &= I(U^{i+1}; Y, U^{1:i}). \end{aligned}$$

At the same time, Theorem 1 implies that $U^{i+1} \rightarrow (X, U^{1:i}) \rightarrow Y$, and so also $U^{i+1} \rightarrow (X, U^{1:i}) \rightarrow (Y, U^{1:i})$. Hence, we have $\mathcal{L}_{U^{i+1}|(Y, U^{1:i})} \subseteq \mathcal{L}_{U^{i+1}|(X, U^{1:i})}$. So, as the blocklength goes to infinity, the rate of communication converges to

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{|Z|}{N} - I(U^{i+1}; Y, U^{1:i}) &= I(U^{i+1}; X, U^{1:i}) - I(U^{i+1}; Y, U^{1:i}) \\ &= (H(U^{i+1}) - H(U^{i+1} | X, U^{1:i})) - (H(U^{i+1}) - H(U^{i+1} | Y, U^{1:i})) \\ &= H(U^{i+1} | Y, U^{1:i}) - H(U^{i+1} | X, U^{1:i}) \\ &= H(U^{i+1} | Y, U^{1:i}) - H(U^{i+1} | X, U^{1:i}, Y) \\ &= I(X; U^{i+1} | Y, U^{1:i}) \end{aligned} \tag{19}$$

which is consistent with (1). Eq. (19) is justified by the fact that $U^{i+1} \rightarrow (X, U^{1:i}) \rightarrow Y$ is a Markov chain.

The claim for the case when $i+1$ is even follows similarly. \square

4.4. Generalization of Lemmas 4 and 5 to multiple rounds. In this section we show that the joint distributions of both $\mathbf{U}_A^{1:t}, \bar{X}, \bar{Y}$ and $\mathbf{U}_B^{1:t}, \bar{X}, \bar{Y}$ are close to $P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}$, and that $\mathbf{U}_A^{1:t} = \mathbf{U}_B^{1:t}$ holds true with probability close to 1. This is accomplished by extending Lemmas 4 and 5 to the case of $t > 1$. We again face the same technical difficulties as discussed in the beginning of Sect. 4, but fortunately it is possible to leverage the proofs of these lemmas to complete the argument.

Let $Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}}$ and $Q_{\mathbf{U}_B^{1:t} \bar{X} \bar{Y}}$ be the empirical distributions induced by the sequence generation and communication protocols explained in Section 4.3. More formally, let

$$\begin{aligned} Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}}(\mathbf{u}_A^{1:t}, \mathbf{v}_A^{1:t}, \bar{x}, \bar{y}) &= \prod_{j=1}^N P_{X,Y}(x^j, y^j) \prod_{i=0}^{t-1} \mathbb{1}(\bar{u}_A^{i+1} G_N = \bar{v}_A^{i+1}) \\ &\times \prod_{i=0}^{t-1} \prod_{j=1}^N Q_{(V_A^{i+1})^j | (V_A^{i+1})^{1:j-1}, (\bar{X}, \mathbf{U}_A^{1:i})}((v_A^{i+1})^j | (v_A^{i+1})^{1:j-1}, (\bar{x}, \mathbf{u}^{1:i})) \end{aligned}$$

and let $Q_{\mathbf{U}_B^{1:t} \bar{X} \bar{Y}}(\mathbf{u}_B^{1:t}, \mathbf{v}_B^{1:t}, \bar{x}, \bar{y})$ be defined similarly. Here, $\mathbf{V}_A^{1:t} \triangleq (\bar{V}_A^1, \dots, \bar{V}_A^t)$, $\mathbf{U}_A^{1:t} \triangleq (\bar{U}_A^1, \dots, \bar{U}_A^t)$ and the notation $\mathbf{V}_B^{1:t}$ and $\mathbf{U}_B^{1:t}$ has a similar meaning.

Lemma 7. *For any $\beta_3 < \beta \in (0, 1/2)$, starting with some N we have*

$$\Pr \{ \mathbf{U}_A^{1:t} = \mathbf{U}_B^{1:t} \} = 1 - O(2^{-N^{\beta_3}}) \tag{20}$$

$$\|Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}\|_1 = O(2^{-N^{\beta_3}}) \tag{21}$$

$$\|Q_{\mathbf{U}_B^{1:t} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}\|_1 = O(2^{-N^{\beta_3}}). \tag{22}$$

Proof. The proof proceeds by induction on the number of rounds. From the Lemmas 4 and 5 we know that (20)-(22) hold true for $t = 1$. Let us assume that they hold for $t = i$ and prove them for $t = i + 1$. If $i + 1$ is odd, then the transmitting party is Terminal A. Then, from the induction hypothesis

$$\|Q_{\mathbf{U}_A^{1:i} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:i} \bar{X} \bar{Y}}\|_1 = O(2^{-N^{\beta_3}}) \quad (23)$$

one can prove (23) for $i + 1$ in the same way as done in the proof of Lemma 4 in Section 4.1 with the only difference that the Markov chain $U^{i+1} \rightarrow (X, U^{1:i}) \rightarrow Y$ is used instead of $U^1 \rightarrow X \rightarrow Y$. Further, we use the induction hypothesis

$$\|Q_{\mathbf{U}_B^{1:i} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:i} \bar{X} \bar{Y}}\|_1 = O(2^{-N^{\beta_3}}) \quad (24)$$

$$\Pr\{\mathbf{U}_A^{1:i} = \mathbf{U}_B^{1:i}\} = 1 - O(2^{-N^{\beta_3}}) \quad (25)$$

and the triangle inequality

$$\|Q_{\mathbf{U}_B^{1:i+1} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:i+1} \bar{X} \bar{Y}}\|_1 \leq \|Q_{\mathbf{V}_B^{1:i} \bar{X} \bar{Y}} - P_{\mathbf{V}^{1:i} \bar{X} \bar{Y}}\|_1 + \|\hat{Q}_{\mathbf{V}_B^{1:i+1} \bar{X} \bar{Y}} - P_{\mathbf{V}^{1:i+1} \bar{X} \bar{Y}}\|_1 \quad (26)$$

where

$$\hat{Q}_{\mathbf{V}_B^{1:i+1} \bar{X} \bar{Y}}(\mathbf{v}^{1:i+1}, \bar{x}, \bar{y}) = Q_{\mathbf{V}_B^{i+1} | \mathbf{V}_B^{1:i} \bar{X} \bar{Y}}(\mathbf{v}^{i+1} | \mathbf{v}^{1:i}, \bar{x}, \bar{y}) P_{\mathbf{V}^{1:i} \bar{X} \bar{Y}}(\mathbf{v}^{1:i}, \bar{x}, \bar{y})$$

similarly to (87), to observe that one can prove (24), (25) for $i + 1$ in the same way as in the proof of Lemma 5. This is because together with (24), (25), the inequality given in (26) makes it possible to reduce the analysis of Round $i + 1$ to that of Round 1. Here again we rely on the Markov condition $U^{i+1} \rightarrow (X, U^{1:i}) \rightarrow Y$ instead of $U^1 \rightarrow X \rightarrow Y$. The case of $i + 1$ even is handled similarly. In that case, we have the Markov chain condition $U^{i+1} \rightarrow (Y, U^{1:i}) \rightarrow X$ instead of $U^{i+1} \rightarrow (X, U^{1:i}) \rightarrow Y$. This completes the induction argument. \square

4.5. Computing the functions. Let us show that the functions $f_A(\bar{x}, \bar{y})$, $f_B(\bar{x}, \bar{y})$ can be computed based on the communication between the terminals described in the previous sections. Using Lemma 7, we prove that Terminals A and B compute their respective values of f_A and f_B respectively with probability close to one.

Proposition 8. *For Terminal A, there exists a $\tilde{Z}_A^{1:N}$ depending on \bar{x} and $\mathbf{u}^{1:t}$ such that for all $0 < \beta_\tau < \beta < 1/2$, we have*

$$\Pr\{\tilde{Z}_A^{1:N} = f_A(\bar{X}, \bar{Y})\} = 1 - O(2^{-N^{\beta_\tau}}) \quad (27)$$

starting from some N . Similarly, for Terminal B, there exists a $\tilde{Z}_B^{1:N}$ depending on \bar{y} and $\mathbf{u}^{1:t}$ such that

$$\Pr\{\tilde{Z}_B^{1:N} = f_B(\bar{X}, \bar{Y})\} = 1 - O(2^{-N^{\beta_\tau}}) \quad (28)$$

starting from some N . Moreover, the computation of $\tilde{Z}_A^{1:N}$ and $\tilde{Z}_B^{1:N}$ is linear in blocklength.

Proof. The proof relies on the conditional entropy constraints $H(f_A(X, Y) | X, U^{1:t}) = 0$ and $H(f_B(X, Y) | Y, U^{1:t}) = 0$ in (1). First observe that these constraints easily extend to the case of N independent repetitions, i.e., that we have

$$H(f_A(\bar{X}, \bar{Y}) | \bar{X}, \mathbf{U}^{1:t}) = 0 \quad (29)$$

$$H(f_B(\bar{X}, \bar{Y}) | \bar{Y}, \mathbf{U}^{1:t}) = 0. \quad (30)$$

Then, define $\tilde{Z}_A^{1:N}$ and $\tilde{Z}_B^{1:N}$ as the values which satisfy

$$P_{f_A(\bar{X}, \bar{Y}) | \bar{X}, \mathbf{U}^{1:t}}(\tilde{Z}_A^{1:N} | \bar{X}, \mathbf{U}^{1:t}) = 1$$

$$P_{f_B(\bar{X}, \bar{Y}) | \bar{Y}, \mathbf{U}^{1:t}}(\tilde{Z}_B^{1:N} | \bar{Y}, \mathbf{U}^{1:t}) = 1$$

Note that the computation of both $\tilde{Z}_A^{1:N}$ and $\tilde{Z}_B^{1:N}$ is linear in blocklength. From (21)-(22) and the conditional entropy constraints (29)-(30), it follows that $\tilde{Z}_A^{1:N}$ and $\tilde{Z}_B^{1:N}$ exist with probability $1 - O(2^{-N^{\beta_3}})$. The rest of proof is devoted to show (27) and (28). For that purpose, we first rewrite (29) and (30) as

$$H(f_A(\bar{X}, \bar{Y}), \bar{X}, \mathbf{U}^{1:t}) - H(\bar{X}, \mathbf{U}^{1:t}) = 0 \quad (31)$$

$$H(f_B(\bar{X}, \bar{Y}), \bar{Y}, \mathbf{U}^{1:t}) - H(\bar{Y}, \mathbf{U}^{1:t}) = 0. \quad (32)$$

Let $H_Q(f_A(\bar{X}, \bar{Y}), \bar{X}, \mathbf{U}_A^{1:t})$ refer to the entropy defined by the distribution $Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}}$. For a sufficiently large N and for all $0 < \beta_4 < \beta_3 < 1/2$ we have

$$|H_Q(f_A(\bar{X}, \bar{Y}), \bar{X}, \mathbf{U}_A^{1:t}) - H(f_A(\bar{X}, \bar{Y}), \bar{X}, \mathbf{U}^{1:t})| \leq -\|Q_{f_A(\bar{X}, \bar{Y}) \bar{X} \mathbf{U}_A^{1:t}} - P_{f_A(\bar{X}, \bar{Y}) \bar{X} \mathbf{U}^{1:t}}\|_1 \log_2 \frac{\|Q_{f_A(\bar{X}, \bar{Y}) \bar{X} \mathbf{U}_A^{1:t}} - P_{f_A(\bar{X}, \bar{Y}) \bar{X} \mathbf{U}^{1:t}}\|_1}{|\mathcal{Z}_A|^N |\mathcal{X}|^N 2^{Nt}} \quad (33)$$

$$\leq -\|Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}\|_1 \log_2 \frac{\|Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}\|_1}{|\mathcal{Z}_A|^N |\mathcal{X}|^N 2^{Nt}} \quad (34)$$

$$\begin{aligned} &\leq N(t + \log_2 |\mathcal{X}| + \log_2 |\mathcal{Z}_A|) \|Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}\|_1 \\ &\quad - \|Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}\|_1 \log_2 (\|Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}\|_1) \\ &= O(N2^{-N\beta_3}) + O(N\beta_3 2^{-N\beta_3}) \end{aligned} \quad (35)$$

$$= O(2^{-N\beta_4}) \quad (36)$$

where (33) uses a standard estimate (e.g., [7, Theorem 17.3.3]), (34) is implied by the inequality

$$\|Q_{\mathbf{U}_A^{1:t} \bar{X} \bar{Y}} - P_{\mathbf{U}^{1:t} \bar{X} \bar{Y}}\|_1 \geq \|Q_{f_A(\bar{X}, \bar{Y}) \bar{X} \mathbf{U}_A^{1:t}} - P_{f_A(\bar{X}, \bar{Y}) \bar{X} \mathbf{U}^{1:t}}\|_1$$

and (35) is a consequence of (21). In the calculations above, $|\mathcal{Z}_A|$ denotes the cardinality of the range of f_A . Similarly to (36), we observe that

$$|H_Q(\bar{X}, \mathbf{U}_A^{1:t}) - H(\bar{X}, \mathbf{U}^{1:t})| = O(2^{-N\beta_4}). \quad (37)$$

Now estimates (36), (37) and the equality (31) imply that

$$H_Q(f_A(\bar{X}, \bar{Y})|\bar{X}, \mathbf{U}_A^{1:t}) = O(2^{-N\beta_4}) \quad (38)$$

for all $0 < \beta_4 < \beta < 1/2$ and N large enough.

On account of (22) and (32) this derivation can be repeated for f_B as well, and we obtain

$$H_Q(f_B(\bar{X}, \bar{Y})|\bar{X}, \mathbf{U}_B^{1:t}) = O(2^{-N\beta_4}). \quad (39)$$

Expanding (38), we get

$$\sum_{\bar{x}, \mathbf{u}_A^{1:t}} Q_{\bar{X}, \mathbf{U}_A^{1:t}}(\bar{x}, \mathbf{u}_A^{1:t}) \sum_{\bar{z}_A \in \mathcal{Z}_A^N} Q_{f_A(\bar{X}, \bar{Y})|\bar{X}, \mathbf{U}_A^{1:t}}(\bar{z}_A|\bar{x}, \mathbf{u}_A^{1:t}) \log_2 \frac{1}{Q_{f_A(\bar{X}, \bar{Y})|\bar{X}, \mathbf{U}_A^{1:t}}(\bar{z}_A|\bar{x}, \mathbf{u}_A^{1:t})} = O(2^{-N\beta_4}) \leq 2^{-N\beta_5} \quad (40)$$

where $\beta_5 < \beta_4$ can be chosen arbitrarily close to β_4 provided that N is sufficiently large.

Now let us define the set

$$S = \left\{ (\bar{x}, \mathbf{u}_A^{1:t}) : \sum_{\bar{z}_A \in \mathcal{Z}_A^N} Q_{f_A(\bar{X}, \bar{Y})|\bar{X}, \mathbf{U}_A^{1:t}}(\bar{z}_A|\bar{x}, \mathbf{u}_A^{1:t}) \log_2 \frac{1}{Q_{f_A(\bar{X}, \bar{Y})|\bar{X}, \mathbf{U}_A^{1:t}}(\bar{z}_A|\bar{x}, \mathbf{u}_A^{1:t})} > \sqrt{2^{-N\beta_5}} \right\}.$$

Using (40) we obtain

$$\sum_{(\bar{x}, \mathbf{u}_A^{1:t}) \in S} Q_{\bar{X}, \mathbf{U}_A^{1:t}}(\bar{x}, \mathbf{u}_A^{1:t}) \leq \sqrt{2^{-N\beta_5}}$$

and therefore with probability at least $1 - 2^{-\frac{N\beta_5}{2}}$ Terminal A can find a value $\hat{Z}_A^{1:N}$ such that

$$\frac{1 - Q_{f_A(\bar{X}, \bar{Y})|\bar{X}, \mathbf{U}_A^{1:t}}(\hat{Z}_A^{1:N}|\bar{x}, \mathbf{u}_A^{1:t})}{(e-1)\ln 2} \leq 2^{-\frac{N\beta_5}{2}}. \quad (41)$$

Here we have used the inequality $(1-x)/(e-1) \leq -x \ln x$, $e^{-1} \leq x \leq 1$ which can be proved by differentiation. From (41) we obtain

$$Q_{f_A(\bar{X}, \bar{Y})|\bar{X}, \mathbf{U}_A^{1:t}}(\hat{Z}_A^{1:N}|\bar{x}, \mathbf{u}_A^{1:t}) \geq 1 - \ln 2 (e-1) 2^{-\frac{N\beta_5}{2}}. \quad (42)$$

Hence, from (42), we conclude that Terminal A can calculate the function $f_A(\bar{X}, \bar{Y})$ correctly with probability at least

$$(1 - 2^{-\frac{N\beta_5}{2}}) \left[1 - \ln 2 (e-1) 2^{-\frac{N\beta_5}{2}} \right] = 1 - O(2^{-N\beta_6}).$$

Repeating the derivation above starting with (39), we prove that Terminal B can find a value $\hat{Z}_B^{1:N}$ and thus calculate the function $f_B(\bar{X}, \bar{Y})$ correctly with probability $1 - O(2^{-N^{\beta_6}})$. Lastly, using (21)-(22) again, we observe that

$$\begin{aligned}\Pr\{\tilde{Z}_A^{1:N} = \hat{Z}_A^{1:N}\} &= 1 - O(2^{-N^{\beta_3}}) \\ \Pr\{\tilde{Z}_B^{1:N} = \hat{Z}_B^{1:N}\} &= 1 - O(2^{-N^{\beta_3}}).\end{aligned}$$

Hence, we conclude

$$\begin{aligned}\Pr\{f_A(\bar{X}, \bar{Y}) = \tilde{Z}_A^{1:N}\} &= 1 - O(2^{-N^{\beta_6}}) - O(2^{-N^{\beta_3}}) = 1 - O(2^{-N^{\beta_7}}) \\ \Pr\{f_B(\bar{X}, \bar{Y}) = \tilde{Z}_B^{1:N}\} &= 1 - O(2^{-N^{\beta_6}}) - O(2^{-N^{\beta_3}}) = 1 - O(2^{-N^{\beta_7}})\end{aligned}$$

as desired. \square

The proof that the rate region (1) can be achieved using polar coding is now complete.

In conclusion we note that all the proofs presented in Sections 4.1, 4.3, and 4.4 can be extended to the case when the auxiliary random variables U^1, U^2, \dots, U^t are not binary using for instance the methods in [19], [18]. Another alternative is viewing U^i as the composition of bits $U^{i,1}, \dots, U^{i,r}$ and dividing each round of communication into r steps each of which are responsible from the conditional distribution $Q(u^{i,k} | u^{1:i-1}, u^{(i,1):(i,k-1)}, \bar{x}), k = 1, 2, \dots, r$. We confine ourselves to this brief remark, leaving the details to the reader.

4.6. An example of interactive function computation. As observed earlier, to complete the description of the communication scheme we need to specify the random variables U^1, U^2, \dots, U^t that satisfy the Markov chain conditions and conditional entropy equalities in (1). The description of these random variables depends on the function being computed and is studied on a case-by-case basis.

Following [12] consider the example in which Terminals A and B observe binary random sequences with $X \sim \text{Ber}(p)$, $Y \sim \text{Ber}(q)$, where X and Y are independent. Suppose that both terminals need to compute the AND function, i.e., $f_A(x, y) = f_B(x, y) = x \wedge y$. We can assume that there exist random variables $(V_x, V_y) \sim \text{Uniform}([0, 1]^2)$ such that $X \triangleq \mathbb{1}_{[1-p, 1]}(V_x)$ and $Y \triangleq \mathbb{1}_{[1-q, 1]}(V_y)$. Further, let $\Gamma \triangleq \{(\alpha(s), \beta(s)), 0 \leq s \leq 1\}$ be a curve defined parametrically with boundary conditions $\alpha(0) = \beta(0) = 0$, $\alpha(1) = 1 - p$ and $\beta(1) = 1 - q$ and let $0 = s_0 < s_1 < \dots < s_{t/2-1} < s_{t/2} = 1$ be a partition of the segment $[0, 1]$. Consider the following t random variables

$$\begin{aligned}U^{2i-1} &\triangleq \mathbb{1}_{[\alpha(s_i), 1] \times [\beta(s_{i-1}), 1]}(V_x, V_y) \\ U^{2i} &\triangleq \mathbb{1}_{[\alpha(s_i), 1] \times [\beta(s_i), 1]}(V_x, V_y)\end{aligned}\tag{43}$$

where $i = 1, \dots, t/2$. In [12] it is shown that for all partitions and curves Γ of the form defined above, random variables (43) satisfy both the Markov chain and the conditional entropy constraints in (1).

Hence, for the AND function, we can construct a polar-coded communication scheme based on (43). In each transmission round, we can construct codes following the partition of the index set $[N]$ as in (8) and (16). For example, according to (16) we have to determine the noiseless and noisy bits of the transmission for the channel with binary input U^{i+1} and output $(X, U^{1:i})$. After $n = \log_2 N$ iterations the size of the output alphabets of the virtual channels obtained will be $2^{N(i+1)} = 2^{2^n(i+1)}$. To simplify the computations involved in the code construction one can rely on the alphabet reduction methods proposed in [20].

Moreover, the choice of random variables according to (43) minimizes the *sum-rate* $\sum_{j=1}^t R_j$ for $t \rightarrow \infty$. (See [13] for the proof.) In [12], it is also shown that

$$R_{\text{sum}, \infty} = h_2(p) + ph_2(q) + p \log_2(q) + p(1-q) \log_2 e < h_2(p) + ph_2(q) = R_{\text{sum}, 2}^A\tag{44}$$

where h_2 is the binary entropy function, $R_{\text{sum}, \infty}$ is the minimum sum-rate as $t \rightarrow \infty$, and $R_{\text{sum}, 2}^A$ is the minimum sum-rate for the case $t = 2$ and it is Terminal A that transmits first. This example shows that for the problem of computing the AND function one can gain by performing several rounds on interactive communication.

5. POLAR CODES FOR COLLOCATED NETWORKS

In this section we consider the multi-terminal function computation problem introduced in Sect. 2.2. We will show that the polar-coded communication scheme introduced above can be modified to achieve the rate region given in Theorem 2.

Let U^1, \dots, U^t be random variables that satisfy the Markov chain conditions and conditional entropy conditions of Theorem 2.

5.1. Communication protocol. Before starting to explain the protocol, we define P as

$$\begin{aligned} & P_{\mathbf{V}^{1:t}, \mathbf{U}^{1:t}, \mathbf{X}^{1:m}}(\mathbf{v}^{1:t}, \mathbf{u}^{1:t}, \mathbf{x}^{1:m}) \\ &= \prod_{i=1}^t \mathbb{1}((u^i)^{1:N} G_N = (v^i)^{1:N}) \prod_{k=1}^N P_{X^{1:m}, U^{1:t}}((x^1)^k, \dots, (x^m)^k, (u^1)^k, \dots, (u^t)^k) \end{aligned} \quad (45)$$

where $\mathbf{x}^{1:m} \triangleq ((x^1)^{1:N}, \dots, (x^m)^{1:N})$, $\mathbf{v}^{1:t} \triangleq ((v^1)^{1:N}, \dots, (v^t)^{1:N})$, and $\mathbf{u}^{1:t} \triangleq ((u^1)^{1:N}, \dots, (u^t)^{1:N})$. Similarly to Section 4, the aim of the communication is to let the terminals generate $\mathbf{U}^{1:t}$ such that the joint distribution of $\mathbf{X}^{1:m}$ and $\mathbf{U}^{1:t}$ is close to $P_{\mathbf{U}^{1:t}, \mathbf{X}^{1:m}}$.

Suppose that the transmission starts with Terminal 1. We again rely on the partition of $[N]$ of the form

$$\left. \begin{aligned} \mathcal{F}_r &= \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1|X^1} \\ \mathcal{F}_d &= \mathcal{L}_{U^1} \\ \mathcal{I} &= \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1|X^1}^c \end{aligned} \right\} \quad (46)$$

similarly to (8). Having observed a realization $(x^1)^{1:N}$, the first terminal finds a sequence $(v^1)^{1:N}$ by sampling from the distribution

$$\begin{aligned} & Q_{(V^1)^i|(V^1)^{1:i-1}, (X^1)^{1:N}}((v^1)^i|(v^1)^{1:i-1}, (x^1)^{1:N}) \\ &= \begin{cases} 1/2, & i \in \mathcal{F}_r \\ P_{(V^1)^i|(V^1)^{1:i-1}, (X^1)^{1:N}}((v^1)^i|(v^1)^{1:i-1}), & i \in \mathcal{F}_d \\ P_{(V^1)^i|(V^1)^{1:i-1}, (X^1)^{1:N}}((v^1)^i|(v^1)^{1:i-1}, (x^1)^{1:N}), & i \in \mathcal{I}. \end{cases} \end{aligned} \quad (47)$$

Based on $(v^1)^{1:N}$ Terminal 1 finds the sequence $(u^1)^{1:N} = (v^1)^{1:N} G_N$ and broadcasts the bits $(v^1)^i, i \in \mathcal{I}$. The remaining terminals including the sink terminal calculate their versions of $(v^1)^i, i \notin \mathcal{I}$ from the conditional distribution

$$Q_{(V^1)^i|(V^1)^{1:i-1}}((v^1)^i|(v^1)^{1:i-1}) = \begin{cases} 1/2, & i \in \mathcal{F}_r, \\ P_{(V^1)^i|(V^1)^{1:i-1}}((v^1)^i|(v^1)^{1:i-1}), & i \in \mathcal{F}_d. \end{cases}$$

Then they find the sequence $(u^1)^{1:N} = (v^1)^{1:N} G_N$ and record the result¹.

Note that for large N the rate of communication converges to $R_1 = \lim_{N \rightarrow \infty} |\mathcal{I}|/N = I(U^1; X^1)$, consistent with (3).

In general, the i^{th} message, $i \in [t]$ is generated and sent by Terminal $j, j = (i-1) \bmod m + 1$. At the start of the i^{th} round of communication we assume that all the terminals have the same $i-1$ sequences $\mathbf{u}^{1:i-1}$, each of which was computed as a result of the previous messages. Terminal j first relies on the partition of $[N]$ given by

$$\left. \begin{aligned} \mathcal{F}_r^i &= \mathcal{L}_{U^i}^c \cap \mathcal{H}_{U^i|X^j, U^{1:i-1}} \\ \mathcal{F}_d^i &= \mathcal{L}_{U^i} \\ \mathcal{I}^i &= \mathcal{L}_{U^i}^c \cap \mathcal{H}_{U^i|X^j, U^{1:i-1}}^c \end{aligned} \right\} \quad (48)$$

and finds computes $(v^i)^{1:N}$ by sampling from the distribution

$$\begin{aligned} & Q_{(V^i)^k|(V^i)^{1:k-1}, (X^j)^{1:N}, \mathbf{U}^{1:i-1}}((v^i)^k|(v^i)^{1:k-1}, (x^j)^{1:N}, \mathbf{u}^{1:i-1}) \\ &= \begin{cases} 1/2, & k \in \mathcal{F}_r^i \\ P_{(V^i)^k|(V^i)^{1:k-1}, (X^j)^{1:N}, \mathbf{U}^{1:i-1}}((v^i)^k|(v^i)^{1:k-1}), & k \in \mathcal{F}_d^i \\ P_{(V^i)^k|(V^i)^{1:k-1}, (X^j)^{1:N}, \mathbf{U}^{1:i-1}}((v^i)^k|(v^i)^{1:k-1}, (x^j)^{1:N}, \mathbf{u}^{1:i-1}), & k \in \mathcal{I}^i. \end{cases} \end{aligned} \quad (49)$$

Then, as usual, Terminal j computes $(u^i)^{1:N} = (v^i)^{1:N} G_N$ and broadcasts the sequence $(v^i)^k, k \in \mathcal{I}^i$, where $\mathcal{I}^i = \mathcal{I}^i \setminus \mathcal{L}_{U^i}^c \cap \mathcal{L}_{U^i|U^{1:i-1}}$. Since $\mathcal{L}_{U^i|U^{1:i-1}} \subseteq \mathcal{L}_{U^i|X^j, U^{1:i-1}}$ implies the inclusion $\mathcal{L}_{U^i}^c \cap \mathcal{L}_{U^i|U^{1:i-1}} \subseteq \mathcal{I}^i$, the rate

¹With small probability the sequences $(u^1)^{1:N}$ computed at different terminals will be different; see also Sect. 5.2 below. Abusing notation, we do not differentiate them below in this section.

of this broadcast converges to

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{|\mathcal{I}'^i|}{N} &= I(U^i; U^{1:i-1}, X^j) - I(U^i; U^{1:i-1}) \\ &= H(U^i | U^{1:i-1}) - H(U^i | U^{1:i-1}, X^j) \\ &= I(X^j; U^i | U^{1:i-1}) \end{aligned}$$

in accordance with (3). Based on the sequence $(v^i)^k, k \in \mathcal{I}'^i$, the remaining terminals determine $(v^i)^k, k \notin \mathcal{I}'^i$ by sampling from the distribution

$$\begin{aligned} Q_{(V^i)^k | (V^i)^{1:k-1}, \mathbf{U}^{1:i-1}}((v^i)^k | (v^i)^{1:k-1}, \mathbf{u}^{1:i-1}) \\ = \begin{cases} 1/2, & k \in \mathcal{F}_r^i \\ P_{(V^i)^k | (V^i)^{1:k-1}}((v^i)^k | (v^i)^{1:k-1}), & k \in \mathcal{F}_d^i \\ P_{(V^i)^k | (V^i)^{1:k-1}, \mathbf{U}^{1:i-1}}((v^i)^k | (v^i)^{1:k-1}, \mathbf{u}^{1:i-1}) & k \in \mathcal{I}^i \setminus \mathcal{I}'^i. \end{cases} \end{aligned} \quad (50)$$

As a result, the remaining terminals acquire their versions of the sequence $(u^i)^{1:N}$.

5.2. The analysis of the protocol. To show that the proposed protocol attains the overall goal of function computation we need to show two facts. First, we should prove in each round the sequences $(u^i)^{1:N}$ found by the receiving terminals with high probability are the same as the sequence computed by the broadcasting terminal. Second, we need to prove that the sequences $\mathbf{u}^{1:N}$ we obtain have a joint distribution with the source sequence which is very close to the distribution P given by (45), making it possible to satisfy the condition $H(f(X^{1:m}) | U^{1:t}) = 0$. This entails the same problem as the one we faced in Section 4.1: namely, to prove one of these facts directly, we need the other one. As in Lemma 5 in Section 4.1, we will prove both statements simultaneously by induction. Similarly to the above, we assume that the terminals are provided with random bits whose indices fall in the subsets $\mathcal{F}_r^1, \dots, \mathcal{F}_r^t$.

Let us introduce some notation. Denote by $(U^l)_j^{1:N}$ the random sequence generated by Terminal $j = (i - 1) \bmod m + 1$ in Round l and by $(U^l)_r^{1:N}$ the sequence computed by Terminal $r \neq j$ after the transmission by Terminal j . Denote by $Q_{\mathbf{U}^{1:t}, \mathbf{X}^{1:m}}$ the joint distribution of the source sequences $\mathbf{x}^{1:m} = ((x^1)^{1:N}, (x^2)^{1:N}, \dots, (x^m)^{1:N})$ and the sequences $\mathbf{u}^{1:t} = ((u^1)^{1:N}, (u^2)^{1:N}, \dots, (u^t)^{1:N})$ generated in the course of the communication. More formally, we define $Q_{\mathbf{U}^{1:t}, \mathbf{X}^{1:m}}$ as the marginal distribution of

$$\begin{aligned} Q_{\mathbf{U}^{1:t}, \mathbf{V}^{1:t}, \mathbf{X}^{1:m}}(\mathbf{u}^{1:t}, \mathbf{v}^{1:t}, \mathbf{x}^{1:m}) &= \prod_{k=1}^N P_{X^{1:m}}((x^1)^k, \dots, (x^m)^k) \prod_{i=1}^t \mathbb{1}((u^i)^{1:N} G_N = (v^i)^{1:N}) \\ &\quad \times \prod_{i=1}^t \prod_{k=1}^N Q_{(V^i)^k | (V^i)^{1:k-1}, ((X^j)^{1:N}, \mathbf{U}^{1:i-1})}((v^i)^k | (v^i)^{1:k-1}, ((x^j)^{1:N}, \mathbf{u}^{1:i-1})) \end{aligned}$$

where $Q_{(V^i)^k | (V^i)^{1:k-1}, ((X^j)^{1:N}, \mathbf{U}^{1:i-1})}((v^i)^k | (v^i)^{1:k-1}, (x^j)^{1:N}, \mathbf{u}^{1:i-1})$ is given in (49).

Lemma 9. For any $\beta_7 < \beta \in (0, 1/2)$ and for all $l \in [t]$, and for all $r \neq j$, starting from some N , we have

$$\Pr\{(U^l)_j^{1:N} = (U^l)_r^{1:N}\} = 1 - O(2^{-N^{\beta_7}}) \quad (51)$$

$$\|Q_{\mathbf{U}^{1:t}, \mathbf{X}^{1:m}} - P_{\mathbf{U}^{1:t}, \mathbf{X}^{1:m}}\|_1 = O(2^{-N^{\beta_7}}) \quad (52)$$

Proof. We begin with the case $t = 1$ in which case (52) takes the form

$$\|Q_{(U^1)^{1:N}, \mathbf{X}^{1:m}} - P_{(U^1)^{1:N}, \mathbf{X}^{1:m}}\|_1 = O(2^{-N^{\beta_7}}). \quad (53)$$

Recall that from Lemma 4 we have the estimate

$$\|Q_{(U^1)^{1:N}, (X^1)^{1:N}} - P_{(U^1)^{1:N}, (X^1)^{1:N}}\|_1 = O(2^{-N^{\beta_1}}). \quad (54)$$

On account of the Markov condition $U^1 \rightarrow X^1 \rightarrow X^{2:m}$ in the statement of Theorem 2, we have

$$\begin{aligned} \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1 | X^1} &= \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1 | X^{1:m}} \\ \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1 | X^1} &= \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1 | X^{1:m}} \end{aligned} \quad (55)$$

Hence for all $i \in \mathcal{I} = \mathcal{L}_{U^1}^c \cap \mathcal{H}_{U^1|X^1}^c$ we have

$$P_{(V^1)^i|(V^1)^{1:i-1},(X^1)^{1:N}}((v^1)^i|(v^1)^{1:i-1},(x^1)^{1:N}) = P_{(V^1)^i|(V^1)^{1:i-1},\mathbf{X}^{1:m}}((v^1)^i|(v^1)^{1:i-1},\mathbf{x}^{1:m}) \quad (56)$$

From (55) and (56), we see that (47) is fully equivalent to the computation which uses $\mathbf{x}^{1:m}$ rather than just $(x^1)^{1:N}$ in the conditional probability for the case $i \in \mathcal{I}$. Therefore, (53) follows from Lemma 4, completing the proof of (52) for $t = 1$. In regards to (51) we note that for $t = 1$ it reduces to a special case of (14) in which $Y^{1:N}$ is unavailable.

Our next step is to generalize (53) to t broadcasts, i.e., to show (52). For that purpose, similarly to the triangle inequality method used in Sections 4.1 and 4.4, we write

$$\|\mathbb{Q}_{\mathbf{U}^{1:i}\mathbf{X}^{1:m}} - \mathbb{P}_{\mathbf{U}^{1:i}\mathbf{X}^{1:m}}\|_1 \leq \|\mathbb{Q}_{\mathbf{U}^{1:i-1}\mathbf{X}^{1:m}} - \mathbb{P}_{\mathbf{U}^{1:i-1}\mathbf{X}^{1:m}}\|_1 + \|\widehat{\mathbb{Q}}_{\mathbf{U}^{1:i}\mathbf{X}^{1:m}} - \mathbb{P}_{\mathbf{U}^{1:i}\mathbf{X}^{1:m}}\|_1 \quad (57)$$

where

$$\begin{aligned} \widehat{\mathbb{Q}}_{\mathbf{U}^{1:i}\mathbf{X}^{1:m}}(\mathbf{u}^{1:i}, \mathbf{x}^{1:m}) &= \mathbb{1}((v^i)^{1:N} G_N = (u^i)^{1:N}) P_{\mathbf{U}^{1:i-1}, \mathbf{X}^{1:m}}(\mathbf{u}^{1:i-1}, \mathbf{x}^{1:m}) \\ &\times \prod_{k=1}^N Q_{(V^i)^k|(V^i)^{1:k-1},(X^j)^{1:N},\mathbf{U}^{1:i-1}}((v^i)^k|(v^i)^{1:k-1},(x^j)^{1:N},\mathbf{u}^{1:i-1}). \end{aligned} \quad (58)$$

Now we are ready to use induction. From (53) we see that (52) is true for $t = 1$. Assume that it is also true for $t = i - 1$. Eq. (57) implies that to prove (52) holds for $t = i$, it is sufficient to show

$$\|\widehat{\mathbb{Q}}_{\mathbf{U}^{1:i}\mathbf{X}^{1:m}} - \mathbb{P}_{\mathbf{U}^{1:i}\mathbf{X}^{1:m}}\|_1 = O(2^{-N^{\beta_7}}). \quad (59)$$

Since the marginal of $\widehat{\mathbb{Q}}$ for $\mathbf{u}^{1:i-1}, \mathbf{x}^{1:m}$ equals P , to show (59) we need to focus on the error introduced by the i^{th} round of sequence generation. Owing to the Markov chain condition $U^i \rightarrow (U^{1:i-1}, X^j) \rightarrow (X^{1:j-1}, X^{j+1:m})$, for all $k \in \mathcal{I}^i = \mathcal{L}_{U^i}^c \cap \mathcal{H}_{U^i|X^j, U^{1:i-1}}^c = \mathcal{L}_{U^i}^c \cap \mathcal{H}_{U^i|\mathbf{X}^{1:m}, U^{1:i-1}}^c$ we have

$$\begin{aligned} &P_{(V^i)^k|(V^i)^{1:k-1},(X^j)^{1:N},\mathbf{U}^{1:i-1}}((v^i)^k|(v^i)^{1:k-1},(x^j)^{1:N},\mathbf{u}^{1:i-1}) \\ &= P_{(V^i)^k|(V^i)^{1:k-1},\mathbf{X}^{1:m},\mathbf{U}^{1:i-1}}((v^i)^k|(v^i)^{1:k-1},\mathbf{x}^{1:m},\mathbf{u}^{1:i-1}) \end{aligned}$$

Therefore (59) follows from Lemma 4. This completes the induction argument for (52).

Finally let us justify the induction step for (51) for $t = i$. For this assume that (51) and (52) hold for $t = i - 1$ and note that the proof follows the steps in the proof of Lemma 5 with no changes. \square

In regards to the function computation, we note that the analysis carried out in Section 4.5, implies that the sink node computes the function $f(\mathbf{X}^{1:m})$ correctly with probability converging to 1 as N goes to infinity. This completes the proof of achievability for the region (4) using the described polar coding scheme.

The analysis presented in this section can be easily modified to account for the case of nonbinary auxiliary random variables U^1, \dots, U^t . The remarks made in the end of Section 4.5 apply to the present case as well.

6. CONCLUSION

In this paper, we have considered the two-terminal interactive function computation problem of [12] and its generalization to many terminals given in [14]. For these problems we designed constructive schemes based on polar codes that achieve the optimal rates established earlier by information-theoretic considerations. The communication scheme designed in this paper supports distributed computation under the rates of data exchange that approach the optimal values.

ACKNOWLEDGMENT: The authors are grateful to their colleague Prakash Narayan who drew their attention to the problems of interactive computation.

APPENDIX A. PROOF OF LEMMA 4

To simplify the notation, in the proof we write $Q(\bar{u}^1, \bar{x}, \bar{y})$, $Q(\bar{v}^1, \bar{x})$ instead of

$$Q_{\bar{U}_A^1 \bar{X} \bar{Y}}(\bar{u}_A^1, \bar{x}, \bar{y}), Q_{\bar{V}_A^1 \bar{X}}(\bar{v}_A^1, \bar{x})$$

etc. and extend this convention to the distributions derived from P as well as the corresponding conditional and marginal distributions. Recall also the notational convention $\bar{X} = X^{1:N}$, $\bar{x} = x^{1:N}$ etc. from Sect. 4.

First let us rewrite $P(\bar{u}^1, \bar{x}, \bar{y})$ as

$$\begin{aligned} P(\bar{u}^1, \bar{x}, \bar{y}) &= \prod_{i=1}^N P_{XYU^1}(x^i, y^i, (u^1)^i) \\ &= \prod_{i=1}^N P_{XY}(x^i, y^i) P_{U^1|X}((u^1)^i | x^i) \end{aligned} \quad (60)$$

$$= P(\bar{x}, \bar{y}) P(\bar{u}^1 | \bar{x}) \quad (61)$$

where (60) is due to $U^1 \rightarrow X \rightarrow Y$. Now note that according to (9) Terminal A has to generate the sequence \bar{u}^1 based only on \bar{x} because it does not have access to \bar{y} . So, for all $\bar{u}^1, \bar{x}, \bar{y}$ it follows that

$$Q(\bar{u}^1, \bar{x}, \bar{y}) = Q(\bar{x}, \bar{y}) Q(\bar{u}^1 | \bar{x}) = P(\bar{x}, \bar{y}) Q(\bar{u}^1 | \bar{x}). \quad (62)$$

Using (61) and (62) we compute

$$\begin{aligned} \sum_{\bar{u}^1, \bar{x}, \bar{y}} |Q(\bar{u}^1, \bar{x}, \bar{y}) - P(\bar{u}^1, \bar{x}, \bar{y})| &= \sum_{\bar{u}^1, \bar{x}, \bar{y}} P(\bar{x}, \bar{y}) |Q(\bar{u}^1 | \bar{x}) - P(\bar{u}^1 | \bar{x})| \\ &= \sum_{\bar{u}^1, \bar{x}} P(\bar{x}) |Q(\bar{u}^1 | \bar{x}) - P(\bar{u}^1 | \bar{x})| \\ &= \sum_{\bar{u}^1, \bar{x}} |Q(\bar{u}^1, \bar{x}) - P(\bar{u}^1, \bar{x})|. \end{aligned} \quad (63)$$

Denote the right-hand side of (63) by $\Delta(P, Q)$. Since Arkan's transform is a one-to-one map between \bar{u}^1 and \bar{v}^1 , we have

$$\sum_{\bar{v}^1, \bar{x}} |Q(\bar{v}^1, \bar{x}) - P(\bar{v}^1, \bar{x})| = \Delta(P, Q). \quad (64)$$

Then from (63) and (64) we conclude that

$$\sum_{\bar{v}^1, \bar{x}} |Q(\bar{v}^1, \bar{x}) - P(\bar{v}^1, \bar{x})| = \|Q_{\bar{U}^1, \bar{X}, \bar{Y}} - P_{\bar{U}^1, \bar{X}, \bar{Y}}\|_1$$

Thus, to prove the lemma it suffices to show that

$$\Delta(P, Q) = \sum_{\bar{v}^1, \bar{x}} |Q(\bar{v}^1, \bar{x}) - P(\bar{v}^1, \bar{x})| = O(2^{-N^{\beta_1}}).$$

Let us write $\Delta(P, Q)$ as

$$\Delta(P, Q) = \sum_{\bar{v}^1, \bar{x}} P(\bar{x}) \left| \prod_{i=1}^N Q((v^1)^i | (v^1)^{1:i-1}, \bar{x}) - \prod_{i=1}^N P((v^1)^i | (v^1)^{1:i-1}, \bar{x}) \right|. \quad (65)$$

Applying the telescoping expansion argument used in Lemma 3.5 of [9], one can bound above the right-hand side of (65) to obtain

$$\begin{aligned} \Delta(P, Q) &\leq \sum_{\bar{x}} P(\bar{x}) \sum_{\bar{v}^1} \sum_{i=1}^N |Q((v^1)^i | (v^1)^{1:i-1}, \bar{x}) - P((v^1)^i | (v^1)^{1:i-1}, \bar{x})| \\ &\quad \times \prod_{j=1}^{i-1} P((v^1)^j | (v^1)^{1:j-1}, \bar{x}) \prod_{j=i+1}^N Q((v^1)^j | (v^1)^{1:j-1}, \bar{x}). \end{aligned} \quad (66)$$

Substituting (9) into (66), we obtain

$$\begin{aligned} \Delta(P, Q) &\leq \sum_{i \in \mathcal{F}_r \cup \mathcal{F}_d} \sum_{(v^1)^{1:i-1}, \bar{x}} \sum_{(v^1)^i=0}^1 |Q((v^1)^i | (v^1)^{1:i-1}, \bar{x}) - P((v^1)^i | (v^1)^{1:i-1}, \bar{x})| P((v^1)^{1:i-1}, \bar{x}) \\ &= 2 \sum_{i \in \mathcal{F}_r} E_P \left| \frac{1}{2} - P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) \right| \\ &\quad + 2 \sum_{i \in \mathcal{F}_d} E_P |P((V^1)^i = 0 | (V^1)^{1:i-1}) - P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X})| \end{aligned} \quad (67)$$

where E_P is a shorthand for the expected value $E_{P_{(V^1)^{1:i-1}, \bar{X}}}$.

Proposition 10. *If $i \in \mathcal{F}_r$, then*

$$E_P \left| \frac{1}{2} - P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) \right| \leq 2^{-\frac{N^\beta}{2} - \frac{1}{2}}. \quad (68)$$

Proof. The proof of Lemma 3.8 of [9] is directly applicable here. We first observe

$$Z((V^1)^i | (V^1)^{1:i-1}, \bar{X}) \quad (69)$$

$$\begin{aligned} &= 2 \sum_{(v^1)^{1:i-1}, \bar{x}} P((v^1)^{1:i-1}, \bar{x}) \sqrt{P((V^1)^i = 0 | (v^1)^{1:i-1}, \bar{x}) P((V^1)^i = 1 | (v^1)^{1:i-1}, \bar{x})} \\ &= 2E_P \left[\sqrt{P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) P((V^1)^i = 1 | (V^1)^{1:i-1}, \bar{X})} \right]. \end{aligned} \quad (70)$$

Making use of the fact that for $i \in \mathcal{F}_r$, Def. (8) implies that $Z((V^1)^i | (V^1)^{1:i-1}, \bar{X}) \geq 1 - 2^{-N^\beta}$, we observe that

$$E_P \left[\frac{1}{2} - \sqrt{P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) P((V^1)^i = 1 | (V^1)^{1:i-1}, \bar{X})} \right] \leq 2^{-N^\beta} / 2.$$

Hence also

$$E_P \left[\frac{1}{4} - P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) P((V^1)^i = 1 | (V^1)^{1:i-1}, \bar{X}) \right] \leq 2^{-N^\beta} / 2.$$

Note that the two probabilities inside the brackets sum to one, so we obtain

$$E_P \left[\frac{1}{2} - P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) \right]^2 \leq 2^{-N^\beta} / 2.$$

Finally, using convexity, we obtain (68), as desired. \square

Proposition 11. *If $i \in \mathcal{F}_d$, then there exists an absolute constant $c \in \mathbb{R}$ such that*

$$E_P |P((V^1)^i = 0 | (V^1)^{1:i-1}) - P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X})| \leq c 2^{-\frac{N^\beta}{2}}.$$

Proof. First note that $i \in \mathcal{F}_d \subseteq \mathcal{L}_{U^1}$ implies $Z((V^1)^i | (V^1)^{1:i-1}) \leq 2^{-N^\beta}$ which in turn implies

$$Z((V^1)^i | (V^1)^{1:i-1}, \bar{X}) \leq 2^{-N^\beta}.$$

Hence for any $a \in (0, 1)$

$$\begin{aligned} &2\sqrt{a(1-a)} \Pr\{a < P((V^1)^i = 0 | (V^1)^{1:i-1}) < 1-a\} \\ &\leq 2E_P \sqrt{P((V^1)^i = 0 | (V^1)^{1:i-1}) P((V^1)^i = 1 | (V^1)^{1:i-1})} \\ &\leq 2^{-N^\beta} \end{aligned}$$

and

$$\begin{aligned} &2\sqrt{a(1-a)} \Pr\{a < P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) < 1-a\} \\ &\leq 2E_P \sqrt{P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) P((V^1)^i = 1 | (V^1)^{1:i-1}, \bar{X})} \\ &\leq 2^{-N^\beta} \end{aligned}$$

follows. In particular, for $a = 2^{-N^\beta}$, we obtain

$$P\left(2^{-N^\beta} < P((V^1)^i = 0 | (V^1)^{1:i-1}) < 1 - 2^{-N^\beta}\right) \leq \frac{1}{2} \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} \quad (71)$$

$$P\left(2^{-N^\beta} < P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) < 1 - 2^{-N^\beta}\right) \leq \frac{1}{2} \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}}. \quad (72)$$

Now, letting $D = [0, 2^{-N^\beta}] \cup [1 - 2^{-N^\beta}, 1]$ we obtain

$$\Pr\left\{P((V^1)^i = 0 | (V^1)^{1:i-1}) \in D \wedge P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) \in D\right\} \geq 1 - \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}}. \quad (73)$$

Our next step will be to show that both the probabilities

$$\Pr\left\{P((V^1)^i = 0 | (V^1)^{1:i-1}) \in [1 - 2^{-N^\beta}, 1] \wedge P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) \in [0, 2^{-N^\beta}]\right\} \quad (74)$$

$$\Pr\left\{P((V^1)^i = 0 | (V^1)^{1:i-1}) \in [0, 2^{-N^\beta}] \wedge P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) \in [1 - 2^{-N^\beta}, 1]\right\} \quad (75)$$

are small. Let $S(i, N)$ be the set of pairs $((v^1)^{1:i-1}, \bar{x})$ accounting for the event in (74).

Write

$$\begin{aligned} & \Pr\{(V^1)^i = 0 | (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \Pr\{(V^1)^i = 1, (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \\ &= \Pr\{(V^1)^i = 1 | (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \\ &\quad \times \Pr\{(V^1)^i = 0 | (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \Pr\{(V^1)^{1:i-1} = (v^1)^{1:i-1}\} \end{aligned}$$

and observe that if the pair $((v^1)^{1:i-1}, \bar{x}) \in S(i, N)$ then the first term on the left is ≈ 1 and the first term on the right is ≈ 0 . This implies that

$$(1 - 2^{-N^\beta}) \Pr\{(V^1)^i = 1, (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \leq 2^{-N^\beta} \Pr\{(V^1)^i = 0, (V^1)^{1:i-1} = (v^1)^{1:i-1}\}. \quad (76)$$

In the same way from (74) we obtain

$$\begin{aligned} & 2^{-N^\beta} \Pr\{(V^1)^i = 1, (V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\} \\ & \geq (1 - 2^{-N^\beta}) \Pr\{(V^1)^i = 0, (V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\}. \end{aligned} \quad (77)$$

From (76), (77) we see that (74) can be bounded above as follows:

$$\begin{aligned} & \sum_{((v^1)^{1:i-1}, \bar{x}) \in S(i, N)} \Pr\{(V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\} \\ &= \sum_{((v^1)^{1:i-1}, \bar{x}) \in S(i, N)} \sum_{(v^1)^i=0}^1 \Pr\{(V^1)^i = (v^1)^i, (V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\} \\ &\leq \left(1 + \frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}\right) \sum_{((v^1)^{1:i-1}, \bar{x}) \in S(i, N)} \Pr\{(V^1)^i = 1, (V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\} \\ &\leq \frac{1}{1 - 2^{-N^\beta}} \sum_{(v^1)^{1:i-1} \in S(i, N)} \Pr\{(V^1)^i = 1, (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \\ &\leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} \sum_{(v^1)^{1:i-1} \in S(i, N)} \Pr\{(V^1)^i = 0, (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \\ &\leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} \Pr\{(V^1)^i = 0\}. \end{aligned} \quad (78)$$

(79)

Similarly, it can be shown that the probability (75) is small. Indeed, let $T(i, N)$ be the set of pairs $((v^1)^{1:i-1}, \bar{x})$ accounting for the event in (75). As in (76), (77), for each $((v^1)^{1:i-1}, \bar{x}) \in T(i, N)$ we have

$$\begin{aligned} 2^{-N^\beta} \Pr\{(V^1)^i = 1, (V^1)^{1:i-1} = (v^1)^{1:i-1}\} &\geq (1 - 2^{-N^\beta}) \Pr\{(V^1)^i = 0, (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \\ (1 - 2^{-N^\beta}) \Pr\{(V^1)^i = 1, (V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\} \\ &\leq 2^{-N^\beta} \Pr\{(V^1)^i = 0, (V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\}. \end{aligned}$$

From these two relations we conclude that (75) can be bounded above as

$$\begin{aligned} &\sum_{((v^1)^{1:i-1}, \bar{x}) \in T(i, N)} \Pr\{(V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\} \tag{80} \\ &= \sum_{((v^1)^{1:i-1}, \bar{x}) \in T(i, N)} \sum_{(v^1)^i=0}^1 \Pr\{(V^1)^i = (v^1)^i, (V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\} \\ &\leq \left(1 + \frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}\right) \sum_{((v^1)^{1:i-1}, \bar{x}) \in T(i, N)} \Pr\{(V^1)^i = 0, (V^1)^{1:i-1} = (v^1)^{1:i-1}, \bar{X} = \bar{x}\} \\ &\leq \frac{1}{1 - 2^{-N^\beta}} \sum_{(v^1)^{1:i-1} \in T(i, N)} \Pr\{(V^1)^i = 0, (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \\ &\leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} \sum_{(v^1)^{1:i-1} \in T(i, N)} \Pr\{(V^1)^i = 1, (V^1)^{1:i-1} = (v^1)^{1:i-1}\} \\ &\leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} \Pr\{(V^1)^i = 1\}. \tag{81} \end{aligned}$$

Substituting (79) and (81) in (73), we observe that

$$\Pr\left\{|P((V^1)^i = 0|(V^1)^{1:i-1}) - P((V^1)^i = 0|(V^1)^{1:i-1}, \bar{X})| \leq 2^{-N^\beta}\right\} \geq 1 - \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} - \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2}.$$

Let ξ be the random variable in the brackets, and note that $\Pr\{\xi \in [0, 1]\} = 1$. Then use the fact that

$$E\xi \leq 2^{-N^\beta} \Pr(\xi \leq 2^{-N^\beta}) + \Pr(\xi > 2^{-N^\beta}) \leq 2^{-N^\beta} + \Pr(\xi > 2^{-N^\beta}).$$

This translates into

$$E_P |P((V^1)^i = 0|(V^1)^{1:i-1}) - P((V^1)^i = 0|(V^1)^{1:i-1}, \bar{X})| \leq \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} + \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} + 2^{-N^\beta}. \tag{82}$$

which completes the proof of Proposition 11. \square

Combining Propositions 10 and 11 with (67), we obtain

$$\|Q_{\bar{U}_A^1 \bar{X} \bar{Y}} - P_{\bar{U}^1 \bar{X} \bar{Y}}\|_1 = \Delta(P, Q) = O(N2^{-\frac{N^\beta}{2}})$$

which proves Lemma 4.

APPENDIX B. PROOF OF LEMMA 5

We prove (13) and (14) by induction on i , using the following forms of these relations for a given value of i :

$$\|Q_{(U_B^1)^{1:i} \bar{X} \bar{Y}} - P_{(U^1)^{1:i} \bar{X} \bar{Y}}\|_1 = O(2^{-N^{\beta/2}}) \tag{83}$$

$$\Pr\{(V_A^1)^{1:i} = (V_B^1)^{1:i}\} = 1 - O(2^{-N^{\beta/2}}). \tag{84}$$

To prove the induction base, note that there are four different possibilities for $i = 1$ which may be contained in any of the sets $\mathcal{F}_r, \mathcal{F}_d, \mathcal{I} \setminus \mathcal{I}'$, and \mathcal{I}' ; see (8), (10).

- (1) If $1 \in \mathcal{F}_r$, then Terminals A and B will make the same decision with probability 1, i.e., $\Pr \{(V_A^1)^1 = (V_B^1)^1\} = 1$. This is because we assume that the terminals share a common randomness to decide $(v_A^1)^i$ and $(v_B^1)^i$, $i \in \mathcal{F}_r$. To prove (83), note that the Markov condition $U^1 \rightarrow X \rightarrow Y$ implies that $\bar{U}^1 \rightarrow \bar{X} \rightarrow \bar{Y}$, which implies that $\bar{V}^1 \rightarrow \bar{X} \rightarrow \bar{Y}$ and finally $(V^1)^1 \rightarrow \bar{X} \rightarrow \bar{Y}$. We use this in the following calculation:

$$\begin{aligned} \|Q_{(V_B^1)^1 \bar{X} \bar{Y}} - P_{(V^1)^1 \bar{X} \bar{Y}}\|_1 &= \sum_{\bar{x}, \bar{y}} \sum_{v^1=0}^1 |Q_{(V_B^1)^1 \bar{X} \bar{Y}}(v^1 | \bar{x}, \bar{y}) \\ &\quad - P_{(V^1)^1 \bar{X} \bar{Y}}(v^1 | \bar{x}, \bar{y})| P_{\bar{X} \bar{Y}}(\bar{x}, \bar{y}) \\ &= \sum_{\bar{x}} \sum_{v^1=0}^1 |1/2 - P_{(V^1)^1 | \bar{X}}(v^1 | \bar{x})| P_{\bar{X}}(\bar{x}) \\ &= 2E_P[|1/2 - P((V^1)^1 = 0 | \bar{X})|. \end{aligned}$$

Here the last step follows because $((v_B^1)^i)$'s are uniformly random for $i \in \mathcal{F}_r$, as given by (11). Now using Proposition 10, we obtain (83) for $i = 1$.

- (2) Let $1 \in \mathcal{F}_d = \mathcal{L}_{U^1}$. To prove (83) we use the same argument as above in item (1), using the Markov condition $(V^1)^1 \rightarrow \bar{X} \rightarrow \bar{Y}$ together with Proposition 11.

To prove (84) note that for $i \in \mathcal{F}_d$ we have $Z((V^1)^i | (V^1)^{1:i-1}) \leq 2^{-N^\beta}$; see (8), (5)². Therefore, the random variable $(V_A^1)^i$ is almost deterministic, and the same is true for the random variable $(V_B^1)^i$. This observation is stated formally in (71).

From (71), we see that with probability $1 - \frac{1}{2} \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}}$, Terminals A and B decide $(V_A^1)^1$ and $(V_B^1)^1$ respectively based on independent copies of a Bernoulli random variable that takes the value 0 with probability p such that either $p \leq 2^{-N^\beta}$ or $p \geq 1 - 2^{-N^\beta}$. Therefore, it follows that for sufficiently large N

$$\Pr\{(V_A^1)^1 = (V_B^1)^1\} \geq \left(1 - \frac{1}{2} \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}}\right) (1 - 2p(1 - p)) = 1 - O(2^{-\frac{N^\beta}{2}}) = 1 - O(2^{-N^{\beta/2}}).$$

- (3) Let $1 \in \mathcal{I} \setminus \mathcal{I}' \subseteq \mathcal{L}_{U^1 | Y}$. Estimate (83) will follow from the following proposition.

Proposition 12. *If $i \in \mathcal{I} \setminus \mathcal{I}'$, then for sufficiently large N*

$$E_P[P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{Y}) - P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}, \bar{Y})] = O(2^{-\frac{N^\beta}{2}}).$$

Proof. On account of (6) for $i \in \mathcal{I} \setminus \mathcal{I}' \subseteq \mathcal{L}_{U^1 | Y}$ we obtain $Z((V^1)^i | (V^1)^{1:i-1}, \bar{Y}) \leq 2^{-N^\beta}$, which implies that $Z((V^1)^i | (V^1)^{1:i-1}, \bar{X}, \bar{Y}) \leq 2^{-N^\beta}$.

The remaining part of the proof follows the steps in the proof of Proposition 11. Namely, inequalities (79), (81) and (73) are valid in this case as well, and we again obtain the estimate

$$\begin{aligned} E_P|P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{Y}) - P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}, \bar{Y})| \\ \leq \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} + \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} + 2^{-N^\beta}. \end{aligned}$$

This completes the proof of Proposition 12. □

²If $i = 1$ then $(V^1)^{1:i-1}$ is empty, but below we will use this argument for all i .

Now notice that

$$\begin{aligned}
\|Q_{(V_B^1)^1 \bar{X} \bar{Y}} - P_{(V^1)^1 \bar{X} \bar{Y}}\|_1 &= \sum_{\bar{x}, \bar{y}} \sum_{a=0}^1 |Q_{(V_B^1)^1 \bar{X} \bar{Y}}(a, \bar{x}, \bar{y}) - P_{(V^1)^1 \bar{X} \bar{Y}}(a, \bar{x}, \bar{y})| \\
&= \sum_{\bar{x}, \bar{y}} \sum_{a=0}^1 P_{\bar{X} \bar{Y}}(\bar{x}, \bar{y}) |Q_{(V_B^1)^1 \bar{X} \bar{Y}}(a|\bar{x}, \bar{y}) - P_{(V^1)^1 \bar{X} \bar{Y}}(a|\bar{x}, \bar{y})| \\
&\stackrel{(11)}{=} \sum_{\bar{x}, \bar{y}} \sum_{a=0}^1 P_{\bar{X} \bar{Y}}(\bar{x}, \bar{y}) |P_{(V^1)^1 \bar{Y}}(a|\bar{y}) - P_{(V^1)^1 \bar{X} \bar{Y}}(a|\bar{x}, \bar{y})| \\
&= \sum_{a=0}^1 E_{P_{\bar{X} \bar{Y}}} |P_{(V^1)^1 \bar{Y}}(a|\bar{Y}) - P_{(V^1)^1 \bar{X} \bar{Y}}(a|\bar{X}, \bar{Y})| \\
&= 2E_{P_{\bar{X} \bar{Y}}} |P_{(V^1)^1 \bar{Y}}(0|\bar{Y}) - P_{(V^1)^1 \bar{X} \bar{Y}}(0|\bar{X}, \bar{Y})| \\
&= O(2^{-\frac{N^\beta}{2}})
\end{aligned}$$

where the last estimate follows from Proposition 12. This proves (83).

Regarding (84) note that for $i \in \mathcal{I} \setminus \mathcal{I}'$ we have $Z((V^1)^i | (V^1)^{1:i-1}, \bar{Y}) \leq 2^{-N^\beta}$; see (8), (6). This also implies that $Z((V^1)^i | (V^1)^{1:i-1}, \bar{X}) = Z((V^1)^i | (V^1)^{1:i-1}, \bar{X}, \bar{Y}) \leq 2^{-N^\beta}$. Hence, similarly to (71) and (72), we have

$$\begin{aligned}
P\left(2^{-N^\beta} < P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) < 1 - 2^{-N^\beta}\right) &\leq \frac{1}{2} \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} \\
P\left(2^{-N^\beta} < P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{Y}) < 1 - 2^{-N^\beta}\right) &\leq \frac{1}{2} \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}}.
\end{aligned}$$

Repeating the arguments that led us to conclude that the probabilities in (74) and (75) are small, we obtain

$$\begin{aligned}
&\Pr\left\{P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) \in [1 - 2^{-N^\beta}, 1] \wedge P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{Y}) \in [0, 2^{-N^\beta}]\right\} \\
&+ \Pr\left\{P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{X}) \in [0, 2^{-N^\beta}] \wedge P((V^1)^i = 0 | (V^1)^{1:i-1}, \bar{Y}) \in [1 - 2^{-N^\beta}, 1]\right\} \\
&\leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2}
\end{aligned}$$

Now let us perform a calculation similar to the one in item (2):

$$\begin{aligned}
\Pr\{(V_A^1)^1 = (V_B^1)^1\} &\geq \left(1 - \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} - \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2}\right) (1 - 2^{-N^\beta+1}) \\
&= 1 - O(2^{-\frac{N^\beta}{2}}) \\
&= 1 - O(2^{-N^{\beta/2}})
\end{aligned}$$

This completes the proof of (84).

- (4) If $1 \in \mathcal{I}'$, then using the Markov condition $U^1 \rightarrow X \rightarrow Y$, we observe that (83) holds trivially. Since the bit $(V_A^1)^1$ is known perfectly at terminal B , the same is true for (84).

This establishes the induction base.

Now assume that (83) and (84) hold for some $i \geq 1$. To prove that (83) is also valid for $i + 1$ write

$$\begin{aligned}
& \|Q_{(V_B^1)^{1:i+1} \bar{X} \bar{Y}} - P_{(V^1)^{1:i+1} \bar{X} \bar{Y}}\|_1 \\
&= \sum_{(v^1)^{1:i+1}, \bar{x}, \bar{y}} |Q_B((v^1)^{1:i+1}, \bar{x}, \bar{y}) - P((v^1)^{1:i+1}, \bar{x}, \bar{y})| \\
&\leq \sum_{(v^1)^{1:i+1}, \bar{x}, \bar{y}} Q_B((v^1)^{1:i+1} | (v^1)^{1:i}, \bar{x}, \bar{y}) |Q_B((v^1)^{1:i}, \bar{x}, \bar{y}) - P((v^1)^{1:i}, \bar{x}, \bar{y})| \\
&\quad + \sum_{(v^1)^{1:i+1}, \bar{x}, \bar{y}} P((v^1)^{1:i}, \bar{x}, \bar{y}) |Q_B((v^1)^{1:i+1} | (v^1)^{1:i}, \bar{x}, \bar{y}) \\
&\quad - P((v^1)^{1:i+1} | (v^1)^{1:i}, \bar{x}, \bar{y})| \tag{85}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{(v^1)^{1:i}, \bar{x}, \bar{y}} |Q_B((v^1)^{1:i}, \bar{x}, \bar{y}) - P((v^1)^{1:i}, \bar{x}, \bar{y})| \\
&+ \sum_{(v^1)^{1:i+1}, \bar{x}, \bar{y}} |\hat{Q}_B((v^1)^{1:i+1}, \bar{x}, \bar{y}) - P((v^1)^{1:i+1}, \bar{x}, \bar{y})| \\
&= \|Q_{(V_B^1)^{1:i} \bar{X} \bar{Y}} - P_{(V^1)^{1:i} \bar{X} \bar{Y}}\|_1 + \|\hat{Q}_{(V_B^1)^{1:i+1} \bar{X} \bar{Y}} - P_{(V^1)^{1:i+1} \bar{X} \bar{Y}}\|_1 \tag{86}
\end{aligned}$$

where for simplicity we write $Q_B((v^1)^{1:i+1}, \bar{x}, \bar{y})$ instead of $Q_{(V_B^1)^{1:i+1} \bar{X} \bar{Y}}((v^1)^{1:i+1}, \bar{x}, \bar{y})$, and where

$$\hat{Q}_{(V_B^1)^{1:i+1} \bar{X} \bar{Y}}((v^1)^{1:i+1}, \bar{x}, \bar{y}) = Q_{(V_B^1)^{1:i+1} | (V_B^1)^{1:i} \bar{X} \bar{Y}}((v^1)^{1:i+1} | (v^1)^{1:i}, \bar{x}, \bar{y}) P_{(V^1)^{1:i} \bar{X} \bar{Y}}((v^1)^{1:i}, \bar{x}, \bar{y}) \tag{87}$$

is the distribution whose marginal for $(v^1)^{1:i}, \bar{x}, \bar{y}$ equals $P((v^1)^{1:i}, \bar{x}, \bar{y})$. From the induction hypothesis given by (83), the first term in (86) is small, and so it is enough to prove that

$$\|\hat{Q}_{(V_B^1)^{1:i+1} \bar{X} \bar{Y}} - P_{(V^1)^{1:i+1} \bar{X} \bar{Y}}\|_1 = O(2^{-N^{\beta_2}}).$$

This estimate follows from the arguments made for the case $i = 1$ with no changes.

Regarding (84) we note that the induction hypothesis implies that the distribution $Q_{(V_B^1)^{1:i} \bar{X} \bar{Y}}$ is close to the “true” distribution P by the L_1 distance. Therefore, the arguments given above for each of the cases (1)-(4) for $i = 1$ are applicable to the case of general $i + 1$ given i .

This completes the induction argument and finishes the proof of Lemma 5.

REFERENCES

- [1] E. Arıkan, *Source polarization*, Proc. IEEE Int. Symposium on Information Theory, Austin, TX, June 2010, pp. 899–903.
- [2] E. Arıkan, *Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels*, IEEE Trans. Inform. Theory **55** (2009), no. 7, 3051–3073.
- [3] E. Arıkan and E. Telatar, *On the rate of channel polarization*, Proc. IEEE Int. Sympos. Inform. Theory, Seoul, Korea, June/July 2009, 2009, pp. 1493–1495.
- [4] O. Ayaso, D. Shah, and M. Daleh, *Information theoretic bounds for distributed computation over networks of point-to-point channels*, IEEE Trans. Inform. Theory **56** (2010), no. 12, 6020–6039.
- [5] M. Braverman and A. Rao, *Towards coding for maximum errors in interactive communication*, Proc. 43rd Annual ACM Symposium on Theory of Computing, ACM, 2011, pp. 159–166.
- [6] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, *Secure computation from random error correcting codes*, Eurocrypt 2007, Lecture Notes in Computer Science, vol. 4515, Springer, 2007, pp. 291–310.
- [7] T. Cover and J. A. Thomas, *Elements of information theory*, 2nd ed., Wiley, 2006.
- [8] J. Honda and H. Yamamoto, *Polar coding without alphabet extension for asymmetric models*, IEEE Trans. Inform. Theory **59** (2013), no. 12, 7829–7838.
- [9] S. B. Korada, *Polar codes for channel and source coding*, Ph.D. thesis, EPFL, 2009.
- [10] S. B. Korada, E. Şaşıoğlu, and R. Urbanke, *Polar codes: Characterization of exponent, bounds, and constructions*, IEEE Trans. Inform. Theory **56** (2010), no. 12, 6253–6264.
- [11] J. Körner and K. Marton, *How to encode the modulo-two sum of binary sources*, IEEE Trans. Inform. Theory **25** (1979), no. 2, 219–221.
- [12] N. Ma and P. Ishwar, *Some results on distributed source coding for interactive function computation*, IEEE Trans. Inform. Theory **57** (2011), no. 9, 6180–6195.
- [13] ———, *The infinite-message limit of two-terminal interactive source coding*, IEEE Trans. Inform. Theory **59** (2013), no. 7, 4071–4094.
- [14] N. Ma, P. Ishwar, and P. Gupta, *Interactive source coding for function computation in collocated networks*, IEEE Trans. Inform. Theory **59** (2012), no. 7, 4289–4305.
- [15] M. Mondelli, H. Hassani, and R. Urbanke, *How to achieve the capacity of asymmetric channels*, Proc. 52nd Annual Allerton Conf. Commun. Control Comput., Monticello, IL, 2014, pp. 789–796.

- [16] B. Nazar and M. Gastpar, *Computation over multiple-access channels*, IEEE Trans. Inform. Theory **53** (2007), no. 10, 3498–3516.
- [17] A. Orlitsky and J. R. Roche, *Coding for computing*, IEEE Trans. Inform. Theory **47** (2001), no. 3, 903–917.
- [18] W. Park and A. Barg, *Polar codes for q -ary channels, $q = 2^r$* , IEEE Trans. Inform. Theory **59** (2013), no. 2, 955–969.
- [19] E. Şaşıoğlu, E. Telatar, and E. Arikan, *Polarization for arbitrary discrete memoryless channels*, arXiv:0908.0302.
- [20] I. Tal and A. Vardy, *How to construct polar codes*, IEEE Trans. Inform. Theory **10** (2013), no. 10, 6562–6582.
- [21] H. Tyagi, P. Narayan, and P. Gupta, *When is the function securely computable?*, IEEE Trans. Inform. Theory **57** (2011), no. 10, 6337–6350.